Attachment A

to

RFP No. 4243

Mississippi Division of Medicaid

Interoperability, Data Lake, and APIs (IDA) Program

ITS Project No. 44440

TABLE OF CONTENTS

I. GENERAL

A. How to Respond

1. Beginning with Item 24, label and respond to each outline point in this Attachment A as it is labeled.

2. The State is under the impression that Vendors have read and agree to all items in this RFP. Vendors should take exception to items to which they disagree.

3. The Vendor must respond with "WILL COMPLY" or "EXCEPTION" to each point in this section. In addition, many items in this RFP require detailed and specific responses to provide the requested information. Failure to provide the information requested will result in the Vendor receiving a lower score for that item, or, at the State's sole discretion, being subject to disqualification.

4. "WILL COMPLY" indicates that the Vendor can and will adhere to the requirement. This response specifies that a Vendor or vendor's proposed solution must comply with a specific item or must perform a certain task.

5. If the Vendor cannot respond with "WILL COMPLY", then the Vendor must respond with "EXCEPTION". (See Section V of RFP No. 4243, for additional instructions regarding Vendor exceptions.)

6. Where an outline point asks a question or requests information, the Vendor must respond with the specific answer or information requested.

7. In addition to the above, Vendor must provide explicit details as to the manner and degree to which the proposal meets or exceeds each specification.

B. Mandatory Provisions in Technical Requirements for this RFP

8. Certain items in the technical specifications of this RFP are MANDATORY. Vendors are disallowed explicitly from taking exception to these mandatory requirements, and a proposal that does not meet a mandatory requirement is subject to immediate disqualification.

9. Mandatory requirements are those requirements classified as "**MANDATORY**" in this Attachment A. Meeting a mandatory requirement means the Vendor has provided a detailed response that demonstrates that the Vendor meets the qualifications and experience required and/or the requested functionality exists in the base solution.

10. **MANDATORY:** Attendance at the Vendor Web Conference on Tuesday, October 25, 2022, at 11:00 a.m. Central Time is mandatory for any Vendor who intends to submit an RFP response. No exceptions will be granted to this requirement. Any proposal received from a Vendor who did not have an authorized representative at the Vendor Conference will be rejected.

    a. To access the web conference, Vendors must contact Khelli Reed via e-mail no later than Monday, October 24, 2022, at 12:00 p.m. Central Time to receive dial-in instructions

C. Overview and Background

11. Common Acronyms

Common Acronyms	
ADT	Admit, Discharge, Transfer (HL7)
API	Application Programming Interface
Beneficiary	An individual eligible for medical assistance in accordance with a State's Medicaid Program and who has been certified as eligible by the appropriate agency and has received services. This term is used interchangeably with recipient for the purposes of this RFP
C-CDA	HL7 Version 3 Consolidated-Clinical Document Architecture
CCO	Coordinated Care Organization. This term is synonymous with MCO: Managed Care Organization
CDIP	DOM Program for Clinical Data Interoperability
CFR	Code of Federal Regulations. A codification of the general and permanent rules published in the Federal Register by the Executive departments and agencies of the Federal Government
CHIP	Children's Health Insurance Program
Claim	A request for payment filed with the Fiscal Agent, on a form prescribed by DOM and the Fiscal Agent, by a certified Medicaid provider for Medicaid-covered medical and medically related services rendered on behalf of an eligible Medicaid beneficiary
CMS	Centers for Medicare and Medicaid Services. This is the Federal agency (formerly known as HCFA) responsible for the administration of Medicaid, Medicare, and other health care programs
COO	Coordinated Care Organizations
CPT	Common Procedural Terminology. A unique coding structure scheme for all medical procedures approved by the American Medical Association
CDR	Clinical Data Repository. The CDR is the "As-Is" data store prior to the implementation of the DOM EDL
DDI	Refers to the Design, Development, and Implementation activities of the contract
DHS	Department of Human Services
DOM	Division of Medicaid
DV	Data Virtualization

Common Acronyms	
EHR	Electronic Health Record. A repository (collection) of information related to a patient's health in electronic (computer) form
EDL	Enterprise Data Lake
EMPI	Enterprise Master Person Index
ESB	In the context of this RFP, the existing Division of Medicaid (DOM) Interoperability Platform Enterprise Service Bus (ESB) provided by Gainwell Technologies
ETL	Extract, Transform, Load
EUID	Enterprise Unique Identifier
eVV	Electronic Visit Verification
FHIR	Fast Healthcare Interoperability Resources (HL7)
FY	Fiscal Year: (Federal) - October 1 through September 30 (Mississippi) - July 1 through June 30
FTE	Full Time Equivalent
HCFA	Health Care and Financing Administration
HCPCS	HCFA Common Procedure Coding System. A coding system designed by HCFA (now CMS) that describes the physician and non-physician patient services covered by the Government's Medicaid and Medicare Programs. It is used primarily to report reimbursable services rendered to patients
HIPAA	Health Insurance Portability and Accountability Act of 1996. A Federal law that includes requirements to protect patient privacy, protect security and data integrity of electronic medical records, to prescribe methods and formats for exchange of electronic medical information, and to uniformly identify providers
HIE	Health Information Exchange
HIT	Health Information Technology
HL7	Health Level 7
ICD-9-CM	International Classification of Diseases, 9th Revision Clinical Modification
ICD-10-CM	International Classification of Diseases, 10th Revision Clinical Modification
IHE	Integrating the Healthcare Enterprise

Common Acronyms	
IDA	Interoperability. In the context of this document Interoperability refers to the DOM Interoperability Strategy and Interoperability Tools Project or Vendor
ITS	Mississippi Department of Information Technology Services
IV&V	Independent Verification and Validation. The verification and validation of a software product by an organization that is both technically and managerially separate from the organization responsible for developing the product
LOINC	Logical Observation Identifiers Names and Codes
LTSS	Long Term Services and Support
MCO	Medicaid Managed Care Organization. This term is synonymous with CCO: Coordinated Care Organization
Medicaid	The joint Federal and State medical assistance program that is described in Title XIX of the Social Security Act
Medicaid Trading Partner	An external entity with a real-time, bi-directional data integration with DOM
Medicare	The Federal medical assistance program that is described in Title XVIII of the Social Security Act
MITA	Medicaid Information Technology Architecture
MMIS/MES	Medicaid Management Information System, Medicaid Enterprise System
MPI	Master Patient Index references all patients relating to an area or organization and acting as a source of patient /service user demographic data for other linked services and systems
MRP	MMIS Replacement Project
NCPDP	National Council for Prescription Drug Programs. NCPDP Version 5.1 is the current electronically accepted drug claim format
NDC	National Drug Code
ONC	Office of National Coordinator of Health Information Technology
PDQ	Patient Demographics Query (IHE)
PHI	Protected Health Information
PMBOK	Project Management Body of Knowledge Guide

Common Acronyms	
RESTful	Representational State Transfer (Interface)
RTM	Requirements Traceability Matrix
SNOMED CT	Systematized Nomenclature of Medicine--Clinical Terms
UAT	User Acceptance Test
XDR	Cross-Enterprise Document Reliable Interchange
XDS	Cross Enterprise Data Sharing (IHE)

12. The Mississippi Division of Medicaid (DOM) is the agency responsible for managing the Mississippi Medicaid program and providing access to quality health coverage for vulnerable Mississippians. Medicaid provides health coverage for eligible, low-income populations in Mississippi. DOM has just under 1,000 employees located in a central office, 30 regional offices, with over 70 additional outstations serving the members.

13. DOM has defined a Health Information Technology (HIT) vision and strategy which is detailed in the State Medicaid Health Information Technology Plan (SMHP) published on the DOM website. Two components of the strategy are the subject of this RFP: An Enterprise Data Lake (EDL) and applications that will populate the Data Lake and Use Data extracted from it. This IDA initiative replaces DOM's existing Clinical Data Interoperability Program (CDIP).

14. The CDIP focuses on clinical data exchange between DOM and providers and between DOM and the three Coordinated Care Organizations (CCOs (Magnolia, Molina, and UnitedHealthcare)). CDIP has exchanged millions of clinical records with DOM Trading Partners since its implementation in 2016. These records form the data within a clinical data repository (CDR) that DOM uses to analyze the health of beneficiaries and the performance of DOM programs.

15. DOM's vision is to migrate from the existing CDIP to an overall Interoperability Strategy including an upgrade of the existing CDR to an EDL, as well as new Interoperability Tools to align with Centers for Medicare and Medicaid Services (CMS) rules, requirements, and functionality. This will allow DOM to meet current and future CMS requirements.

16. Vendor's response must include a description of the methodology to be followed in accomplishing each requirement to demonstrate the Vendor's understanding of this RFP.

17. Vendor's response must include information about past performance results for similar work in a Medicaid environment, which include lessons learned from those projects and how they will be applied to this project.

18. DOM is issuing this Request for Proposal (RFP) for multiple components from a qualified Vendor. Vendors should provide sufficient detail as to how their proposal meets or exceeds these requirements:

 a. DOM EDL: Components are further defined in Section II: Functional/Technical Requirements.

b. Data Lake Population tools: Components are further defined in Section II: Functional/Technical Requirements, Item B.

   i. One-time historical load of claims from the MRP system,

   ii. Daily load of claims from the MRP system,

   iii. Daily load of beneficiary data from the DOM Eligibility system,

   iv. Historical load of select Consolidated-Clinical Data Architecture (C-CDAs) clinical data summaries previously received from DOM Trading Partners, and

   v. Daily load of new data received from DOM Trading Partners.

c. Data Lake Control and Management tools: Components are further defined in Section II: Functional/Technical Requirements, Item B.

   i. Security and access control,

   ii. Standard methodologies for access to data in the Data Lake, and

   iii. Audit and quality control tools.

d. Applications: Components are further defined in Section II: Functional/Technical Requirements, Item C.

   i. APIs in support of 2020 CMS and Office of the National Coordinator for Health Information Technology (ONC) Final Rules, and

   ii. General Business Intelligence (BI) tools.

e. Transmission of data to DOM Trading Partners.

f. Integration, operation, Help Desk, and support of the new EDL components, including the interface and data exchange with the new DOM EMPI, which will be provided by Verato. The new DOM EMPI is not in scope for this procurement, as it is currently being contracted with Verato.

g. This RFP defines in detail the requirements for the IDA Solution. High-level goals of the system are:

   i. Promote a data-sharing atmosphere that breaks down functional silos in the state government, provider, and payer communities,

   ii. Provide standards-based access to shared data for future, to-be procured solutions to be added and integrated, such as complex reporting and analytics,

   iii. Stabilize shared data across applications to save time and limit re-work for those who need the data,

   iv. Reduce data quality errors,

   v. Increase confidence in data and promote adoption of future analytics tools to be procured and integrated based on data,

   vi. Save time and energy for DOM employees needing to incorporate shared data in reports,

   vii. Minimize the risk of losing sensitive data,

    viii. Adhere to the CMS Medicaid Information Technology Architecture (MITA) as a modular component and allows for re-use, and

    ix. Conform and meet the requirements in the CMS Final Rule of 2020 (CMS 9115-F), including the adoption of HL7 FHIR.

19. Components detailed in this RFP will replace the existing CDIP project outlined below.
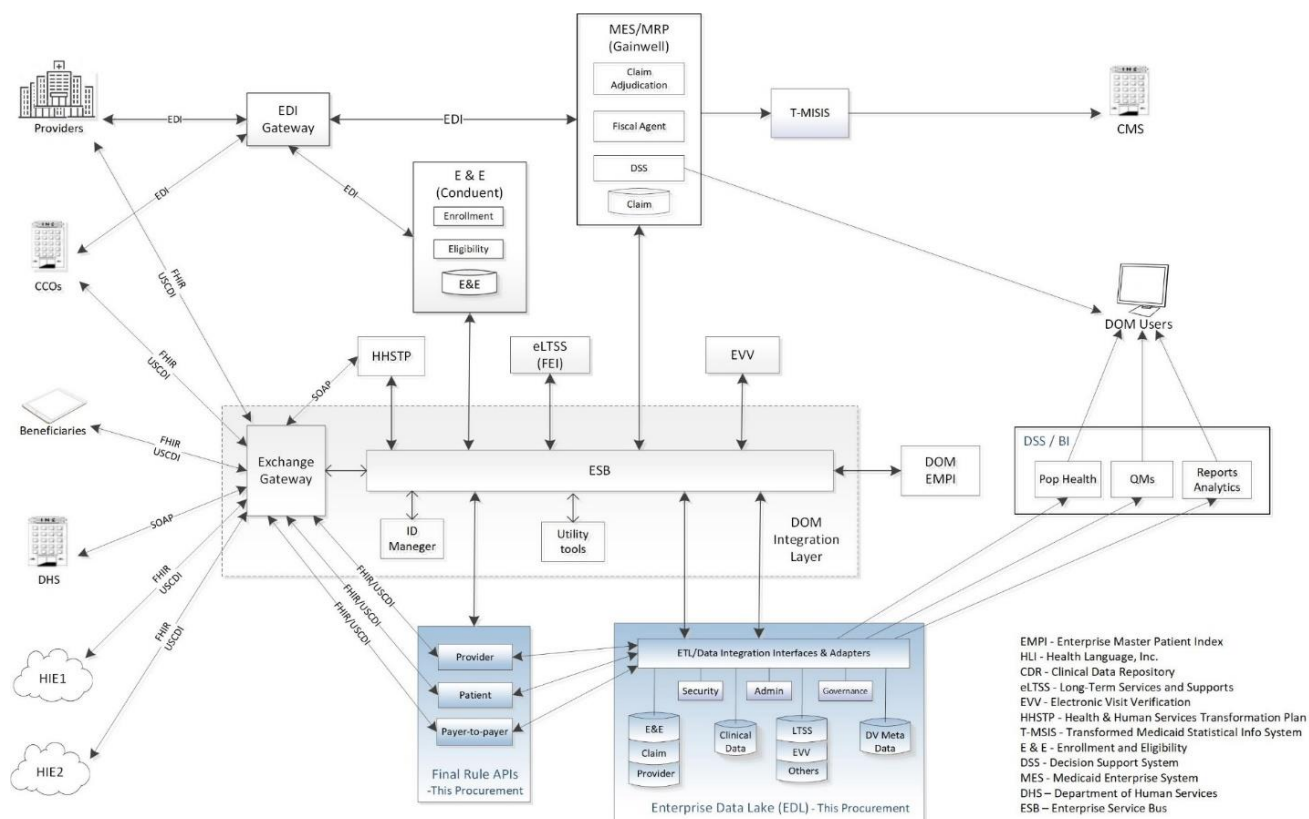
Figure 1: Existing DOM Clinical Data Interoperability Project (CDIP) - Current State
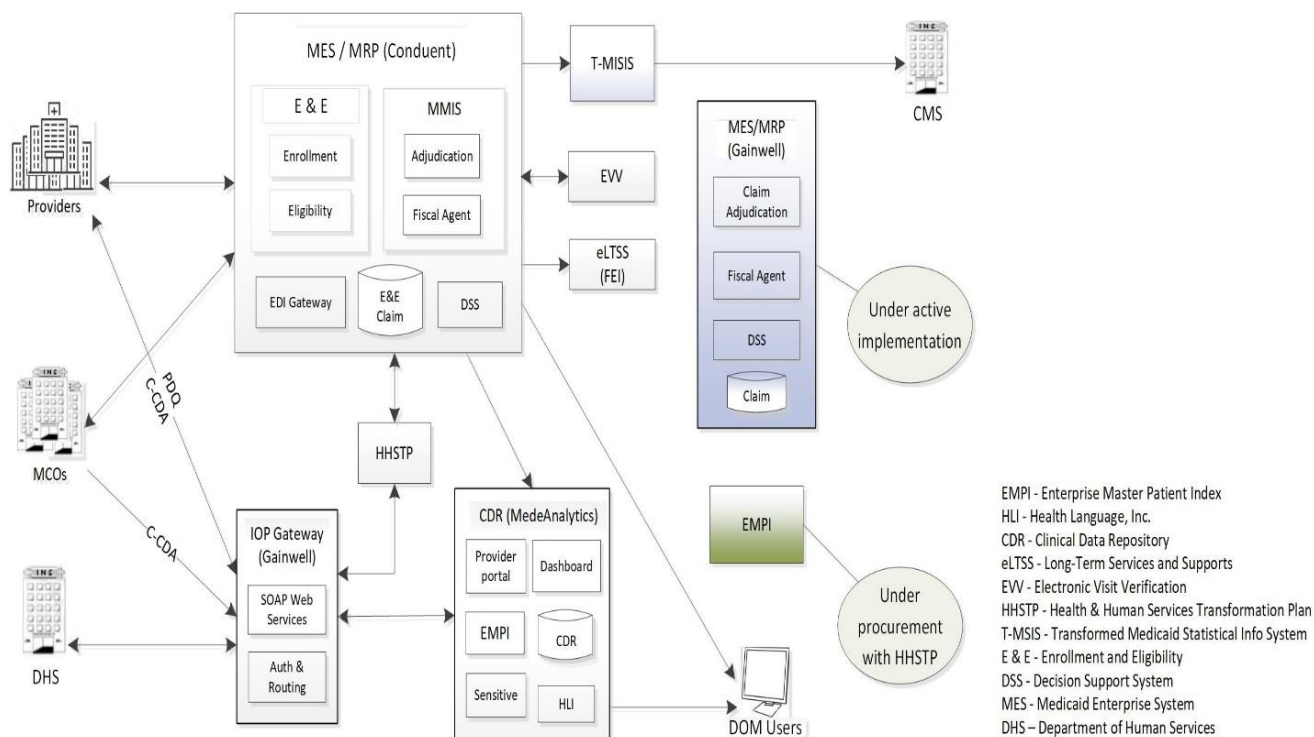
Figure 2: Proposed Interoperability Solution (IDA) Future State

a. The DOM Clinical Data strategy is currently being fulfilled by the DOM CDIP. DOM is issuing this procurement as a replacement of the DOM Medicaid Clinical Infrastructure and program.

b. The core functions of the DOM CDIP are:

   i. Aggregation of Medicaid administrative and clinical data from Medicaid systems, Medicaid CCOs, and provider Electronic Health Records (EHR) systems into the DOM Clinical Data environment,

   ii. Availability of the aggregated Medicaid clinical data for DOM staff to use in analysis to improve beneficiary outcomes and drive healthcare policy in Mississippi, and

   iii. Sharing of aggregated Medicaid clinical data with other DOM Medicaid providers CCOs and Medicaid Trading Partners to improve care of DOM beneficiaries at the point of care.

c. DOM CDIP has two functional, integrated subprojects: the DOM Clinical Data Subproject and the DOM Interoperability Platform Subproject.

d. The current DOM Clinical Data Subproject:

   i. The DOM CDR is made up of two data sources: DOM claims data from the current Medicaid Management Information System (MMIS) system and clinical data that is transmitted via C-CDA from DOM Trading Partners.

ii. The DOM Clinical Data Subproject (CDIP) includes the CDR, a CDIP Medicaid EMPI, and an integrated Medicaid Analytics solution, deployed in a Software as a Service (SaaS) model (Figure 1 – CDIP Current State).

iii. The current DOM Clinical Data Subproject Vendor is MedeAnalytics. This procurement will replace the MedeAnalytics solution.

iv. The current CDIP EMPI Vendor is NextGate, as a subcontractor to MedeAnalytics. The NextGate EMPI will be replaced by the new Verato EMPI solution as the new EMPI solution for DOM applications including the EDL.

v. Figure 1 is the current architectural view of the DOM CDIP. This diagram is for reference only.

vi. The current DOM CDR and CDIP integrated CDIP EMPI functions include the aggregation and sharing of real-time Medicaid clinical data summaries with connected Medicaid Trading Partners. Trading Partners may include Providers, CCOs, Vendors, Health Information Exchanges (HIEs), and State or Federal Agencies.

vii. Clinical integrations are built for bi-directional clinical data exchange directly with the provider's EHR system.

viii. DOM and Medicaid Trading Partners can query and exchange clinical summaries in real time using the C-CDA format. DOM uses the HL7 version 3 C-CDA which is compliant with Stage 2 requirements of the federal Meaningful Use program.

ix. For query and exchange of C-CDAs, DOM uses Integrating Healthcare Enterprise (IHE) standards-based clinical data exchange transactions, such as Patient Demographics Query (PDQ), Provide and Register (PnR), Cross-Enterprise Document Reliable Interchange (XDR), and Cross-Enterprise Document Sharing (XDS.b).

x. There are four connected and live provider Trading Partners (health care systems), and all are using the Epic Care Everywhere interoperability module for their DOM clinical integrations.

xi. There are three CCOs that are live and connected. They are currently in a C-CDA (XDR) send-only mode to DOM. The CCOs are using standards and methodologies for their clinical integrations that are similar to the provider Trading Partners, including XDR and C-CDA.

xii. Medicaid is prohibited from storing clinical data on patients who are not Medicaid beneficiaries. Trading Partners with clinical integrations are asked to send DOM requests for data on active Medicaid beneficiaries only. The existing CDR and EMPI have an integration service that removes non-Medicaid patients and prevents non-Medicaid data from entering the CDR.

xiii. The DOM CDR, upon receipt of a C-CDA, imports the C-CDA into the CDR once the beneficiary has been validated through the EMPI.

xiv. The DOM CDR builds a single, complete C-CDA in real-time from all available data in the CDR upon PDQ request by a Trading Partner and upon validation of the beneficiary through the CDR Integration Service.

xv. The DOM CDR includes a Medicaid Provider Portal, where authorized Medicaid providers can log in, search for, view, and download a C-CDA for an active Medicaid beneficiary. This Provider Portal will be discontinued at the end of the current contract in September 2023 and is not part of this RFP.

xvi. The CDR includes business rules and a business rules engine, sensitivity and terminology services, security, encryption of data, protection of Protected Health Information (PHI), audit trails and audit logs, ongoing support and maintenance of the entire solution, and administrative functionality.

xvii. The DOM CDR has an analytics solution that is a tightly integrated component of the existing CDR. This solution only uses claims-based data and is supported with specialized training services.

e. The current DOM Interoperability Platform (ESB):

   i. The DOM Interoperability Platform includes an ESB that integrates with the existing CDR including the integrated CDIP EMPI. The DOM Interoperability Platform is provided by Gainwell Technologies. The DOM Interoperability Platform (ESB) is outside the scope of the RFP and the new IDA Solution will be required to integrate with the existing solution at the proposed cost.

   ii. All clinical integrations with existing Trading Partners connect through the DOM Interoperability Platform (ESB).

   iii. The DOM Interoperability Platform (ESB) processes all inbound and outbound transactions such as PDQ, PNR, XDS.b, XDR, and C-CDA.

f. The current Analytics solution: Replacement of this component is outside the scope of this RFP.

   i. The DOM Analytics solution relies on administrative and clinical data to produce one-time and ongoing reports on financial and clinical metrics. The reports are built and displayed in a user-friendly, web-based interface. A DOM administrator may add and remove users from the solution and control which reports users may view.

20. DOM has requested below pricing for the development of APIs to support a variety of functions. DOM is separately pursuing the development of these APIs at the earliest possible timeframe. Should these API's have already been developed by DOM with a different vendor, the vendor will be required to integrate these APIs with the new Data Lake solution.

21. Selected Vendors may be required to come onsite for an in-depth presentation on the details of their proposed solution.

22. Vendors are expected to respond to all sections in this RFP. Vendors may propose partners to provide components of the solution; however, the responding Vendor retains responsibility for all components in this RFP. Vendors should understand that DOM anticipates only contracting with the responding/primary Vendor.

23. Prior to contract execution, the awarded Vendor shall be required to execute DOM's Business Associate Agreement (BAA) and may be required to execute Non-Disclosure Agreements with other DOM Vendors. The DOM BAA is incorporated herein as Attachment B.

D. General Requirements

24. **MANDATORY**: All Vendors who respond to this procurement must align their components to share data and identities with the new DOM Enterprise Master Person Index (EMPI), which is currently being procured through RFP No. 4283 and available for review on the ITS website:

    https://www.its.ms.gov/Procurement/Pages/RFPS_Awaiting_tables.aspx.

25. **MANDATORY**: The proposed solution(s) from this RFP must fully integrate with the EMPI (and the EMPI vendor) to allow for seamless, real-time query and exchange of data and identities throughout the solution by using the EMPI for real-time beneficiary identity matching.

26. **MANDATORY**: The new Interoperability, Data Lake, and API (IDA) solution outlined in this procurement must be modular and integrated for seamless, real-time data communication, and interoperability.

27. **MANDATORY**: The proposed solution must include all integration, testing, operational support, data quality services, vendor to vendor communication, and support between components as well as with the EMPI and EMPI vendor (in both the Design, Development, and Implementation (DDI) phase and the ongoing support and maintenance phase) at the cost proposed.

28. **MANDATORY**: The architecture and components of the new Interoperability, Data Lake, and API (IDA) Solution shall be subject to integrate with the DOM Enterprise Service Bus (ESB). All data transmissions with external trading partners should go through existing DOM Interoperability Platform (ESB), provided by Gainwell Technologies, as the connectivity and interoperability broker, and the Vendor should work with Gainwell Technologies and other integration vendors for integration and operations for all data transmissions as well as technical support coordination. All such integration with the ESB or ESB vendor shall be done at no additional cost.

29. The use of offshore and near-shore resources is permitted for development efforts with de-identified data only. All operational aspects, including the location of infrastructure, must be in the continental USA. All operational resources including Technical Support must be in the continental USA. Following go-live, no testing, development, or maintenance work requiring access to production systems or data will be performed offshore. Under no circumstances will PHI, nor security development, coding, or security operations, be moved offshore either for testing purposes or in production.

30. The existing DOM Interoperability Platform ESB provided by Gainwell Technologies, (Gainwell) formerly known as DXC MS LLC, and formerly known as HP Enterprise, is not in scope for this procurement. Gainwell currently maintains connectivity from the DOM Interoperability Platform (ESB) to the external provider Trading Partners, as defined in Figure 1, and will assist the vendors in the migration of these connections from their existing Web Services interfaces to Fast Healthcare Interoperability Resources (FHIR) APIs. All components of the new APIs, IDA solution, and the new EMPI, provided by Verato, shall integrate with the DOM Interoperability Platform (ESB) as the connectivity and interoperability broker, and work with Gainwell for integration and operations for all data transmissions, as well as technical support coordination. It is DOM's vision that in the future, DOM will

procure a new ESB, as a component of the new DOM Integration Layer, and thereby replace the existing DOM Interoperability Platform (ESB). The proposed solution must migrate from the existing DOM Interoperability Platform (ESB) and integrate with the new DOM Integration Layer, including using the Integration Layer's ESB component, Identity Management and Authentication Component, and FHIR services.

31. **MANDATORY:** Vendors must annually attest to meeting the latest version of CMS Minimal Acceptable Risk Standards for Exchanges (MARS-E) and annually attest to a MARS-E compliant environment.

32. **MANDATORY:** Vendors shall assist DOM in meeting CMS certification requirements for their components, including CMS Outcomes Based Certification (OBC), if needed.

33. **MANDATORY:** Vendors shall meet, adhere, and annually report on compliancy with the CMS National Institute of Standards and Technology (NIST) requirements below, and must comply with CMS NIST updates as they occur.

   a. PL-2: System Security and Privacy Plan (SSP)
   b. CM-9: Configuration Management Plan
   c. CP-2: Contingency Plan
   d. CP-4: Contingency Plan Testing and Exercises
   e. IR-8: Incident Response Plan
   f. IR-3: Incident Response Testing and Exercises
   g. AT-3: Security Training
   h. AT-4: Security Training
   i. CA-3: System Interconnections
   j. RA-3: Risk Assessment
   k. AP-1: Authority to Collect
   l. AP-2: Purpose Specification
   m. AR-1: Governance and Privacy Program
   n. AR-2: Privacy Impact and Risk Assessment

34. Vendors who respond to this procurement must provide support and documents, including user guides, with technical specifications to any future analytics Vendors selected by DOM who provide reporting and analytics from all data, including EDL data.

35. The new IDA Project must include all integration, testing, operational support, data quality services, Help Desk and technical support, and Vendor to Vendor communication and support during all phases of the project.

36. Awarded Vendor is expected to work in coordination with any Vendor with which the State has an Agreement.

37. End-of-Contract Transition: DOM requires the awarded Vendor to collaborate with the incumbent Vendor over a 120-day transition period. Transition services must be provided at no additional cost.

   a. Vendor shall provide the End-of-Contract Transition Plan to ensure a quality, smooth, efficient, and timely data transition to DOM or DOM's agents within six

months prior to the end of the Agreement. At a time requested by DOM, the Vendor shall support end-of-contract transition efforts with technical, business, and project support.

38. Vendor shall provide a timely and thorough response to Corrective Action Plans (CAPs), as required by DOM. This includes completion of remediation tasks identified in the CAP and/or Vendor's response to the CAP, which could be initiated to remedy a contractual or Vendor performance issue or as an outcome from an Independent Validation & Verification (IV&V) or other review.

39. The State anticipates signing Service Level Agreements (SLAs) with the awarded Vendor. Exhibit A, *Standard Contract* of the RFP contains detailed SLA information. Vendor should attach samples of existing SLAs.

40. Vendor must affirm all partners and subcontractors will allow DOM to adhere to the State's Enterprise Security Policy, privacy and encryption requirements, and policies including encryption in transit and encryption at rest of all data and protection of PHI.

41. Vendor shall adhere to all current and future CMS and ONC Final Rules, as well as all state and federal requirements for data governance of PHI.

42. Vendor must ensure ongoing services without disruption during the contract transition from the current DOM Clinical Data Program to the new DOM Interoperability Strategy and Interoperability Tools.

43. The proposed solution must include integration, testing, operational support, and data quality services, as well as Help Desk services. If Vendor is working with a partner for their proposed solution, DOM expects Vendors to align, including all Help Desk to Help Desk and Vendor to Vendor communication and support during all phases of the project.

44. Vendor submitting a proposal for the IDA Project will be required to submit a performance bond and include the cost of a performance bond in the RFP Section VIII: *Cost Information Submission*.

45. DOM and ITS acknowledges that the specifications within this RFP are not exhaustive. Rather, they reflect the known requirements that must be met by the proposed system. Vendors must specify, here, what additional components may be needed and are proposed to complete each configuration.

II. FUNCTIONAL/TECHNICAL REQUIREMENTS

A. Start-Up Period Requirements

46. Vendor must complete the start-up period within 30 calendar days from contract execution. During the start-up period, the Vendor must complete the following:

   a. Onsite kick-off meeting must be held within five business days of contract execution. The kick-off meeting materials must cover:
   1. Introduction of personnel from the Vendor team and DOM
   2. Review of work plan
   3. Discussion of assumptions, risks, and issues
   4. Logistics for communications
   5. Additional topics as determined necessary

b. Vendor must fully staff key personnel positions. The State defines key personnel as staff who fill critical project roles and who have the authority and responsibility for planning, directing, and controlling the project activities necessary for a successful project implementation.

c. Vendor must clearly identify all staff considered key personnel. DOM must approve all key personnel.

d. Vendor must submit a Project Management Plan (PMP) and Project Work Plan (PWP) within ten business days of contract execution.

e. Vendor must provide a fully integrated PMP for all aspects of the IDA Project, that include the following sections/sub-plans:

    1. RACI (responsible, accountable, consulted, and informed) Matrix depicting roles and responsibilities of the following for the awarded Vendor and DOM:

        a. Scope Management

        b. Schedule Management

        c. Procurement Management

        d. Quality Management

        e. System Change Management and Configuration Management (software versions and licensing, code libraries, etc.)

        f. Training Management

        g. Staffing Management

        h. Communications Management

        i. Issues and Risk Management

        j. Assumptions

        k. Constraints

    2. Vendor must submit bi-weekly updates to the PWP thereafter.

f. Vendor must submit a Technical Operations Plan (TOP) within 15 business days after contract execution and should support networking and integration.

g. Vendor must provide a technical architecture (hardware, software, net gear, etc.) schematic of its technical infrastructure, roles and responsibilities of staff, methods and procedures for maintenance and operations of Vendor's technical infrastructure, and communications protocols. At a minimum, the TOP must include:

    1. Technical Architecture Schematic

    2. Systems Monitoring

    3. Patch Management

    4. Maintenance Schedule

    5. Points-of-Contact and Backups

    6. Technical Support

    7. Security

    8. HIPAA Compliance

    9. Database Replication

    10. Ad Hoc Reporting Repository

11. Licensing and Warranty Tracking for Hardware and Software
12. Certificate Expiration Date Tracking
13. State Application Performance Monitoring (APM) tool integration into hosting platform
14. Other items as mutually agreed upon

h. Vendor must obtain DOM approval of the TOP, which must include all off-site procedures, locations, and operational protocols.

i. Vendor must submit a Software Deployment Plan within 15 business days of contract execution. Vendor must include <u>in their proposal</u> their approach for Software Deployment.

j. Vendor must implement and maintain a Source Code Version Management and Configuration Control for all code, release notes, etc. so that releases can be rolled back.

k. Vendor must develop, with DOM's input, other project artifacts including:

1. Monthly Progress Reports
2. Bi-weekly PWP updates
3. Maintenance Schedule
4. Tracking tools for:
    a. Hardware Inventory, if applicable
    b. Hardware Maintenance Agreements
    c. Software Licenses
    d. Patches
    e. Technical Infrastructure Changes

l. Vendor must develop a method for diagnosing reported system issues and determining if the issue is a defect. Vendors will be responsible for resolving all defects in the timeframe agreed upon at no additional cost.

m. Vendor must develop a method for deploying the current code into the awarded Vendor's pre-production environment and validating that the code is ready for deployment into the production environment (as documented in the Software Deployment Plan).

n. Vendor must submit a Transition Plan, detailing the transition from the current solution to the new IDA Solution, within 15 business days of contract execution and must include a planned approach for transitioning all contract activities within the specified thirty calendar day timeframe. The plan must include the Vendor's:

1. Proposed approach;
2. Tasks, subtasks, and schedule for activities;
3. Organizational Governance Chart;
4. Project Team Organization Chart;
5. Contract list of all key personnel and executives involved in the project;
6. High-level timeline that encompasses all major project-related activities;

7. Identification of any potential risks or issues to timely implementation, and proposed mitigations; and

8. Detailed description of a process for review, revision, and approval of all deliverables and project artifacts to be approved by DOM.

o. Vendor must ensure that secure protection, backup, and DR measures are in place and operational as a prerequisite to cutover from the current operations and maintenance (O&M) Vendor to the awarded Vendor's hosting and operations of the production components (i.e., for end of Start-Up Period) and for the duration of the contract. Vendor must ensure no loss of data or configuration of the environments.

B. DOM Enterprise Data Lake (EDL)

Vendor must describe in detail how it plans to meet each of the following requirements.

47. DOM seeks the implementation of an EDL to house and serve as a single source for selected DOM data, in a SaaS Model, with full support of the data of HL7 FHIR, C-CDA, and HL7 v2.5, as well as DOM EDI data such as X12 claims data, LTSS data, and other data types and formats. DOM reserves the right add additional datasets in the future and the awarded Vendor will be responsible for incorporating these data sets at no cost to the division.

48. The DOM EDL must have provisions for all data indicated in the following sections of this RFP.

49. The DOM EDL must be scalable to seamlessly house future DOM data requirements.

50. The DOM EDL must be capable of serving data requests both on-demand and on schedule for DOM internal and external customers, including vendors, Trading Partners, and other agencies.

51. Populating the DOM Data Lake:

a. Vendor must describe its approach to inbound data handling. It is DOM's understanding that complex processing is not performed on data as it enters the Data Lake. Data is processed only when it is accessed by external applications. DOM accepts this approach but is open to a hybrid approach where additional processing of data is performed on the way in, with further processing occurring when the data is accessed.

b. Vendor must load the DOM EDL with the following data:

1. One-time historical load of claims from the Medicaid Enterprise System (MES) system.

a. All claims data in the new MES Solution that are dated January 1, 2012, or later, and any claims that DOM identifies as having special timeframes (such as once-in-a-lifetime claims), must be loaded to the DOM EDL.

Vendor: Gainwell
Type of file: Batch via SFTP or FHIR.
Size of current data source: Estimated to be 100 million plus claims.

2. Daily load of claims from the MES system.

   a. On a daily basis, all new or changed claims in the MES solution must be loaded to the DOM EDL.

      Vendor: Gainwell

      Type of file: Batch via SFTP or FHIR.

3. One-off load of claims from the existing MMIS archive.

   a. DOM prefers that data be loaded from the new MES solution if available. However, Vendor may be required to load claims from the legacy MMIS system.

      Vendor: Conduent

      Type of file(s): Batch via SFTP

      Size of current data source: Estimated to be 100 million plus claims.

4. On a weekly basis all new or changed claims in the MMIS system must be loaded to the DOM Data Lake. The existing MMIS system will be replaced by the new MRP solution with a tentative go-live set for October 2022. It is possible that all data and processes will have been migrated to the new MRP solution prior to go-live of the new IDA Solution. In this case, a weekly loads of claims data from MMIS may not be required.

   Vendor: Conduent

   Type of file(s): Batch via SFTP

5. Daily load of beneficiary data from the Eligibility and Enrollment system.

6. Vendor must daily load all new or changed beneficiary data to the Data Lake. Data typically originates in the Enrollment and Eligibility system. This would be the preferred source.

   Vendor: Conduent

   Type of file: Batch via SFTP, real-time via FHIR, One-off load of select C-CDAs previously received from DOM Trading Partners.

7. Beginning in 2016, DOM received, via MedeAnalytics, several million C-CDAs from DOM Trading Partners (Providers and CCOs). Vendor must make available the option to select historic CCDAs based on Provider and/or date received and only input the CCDA's selected.

   Vendor: MedeAnalytics
   Type of file: historical C-CDA

   Size of current data source: As of May 2021, 10 million CCDA's.   This number will increase.

8. Daily load of new data received from DOM Trading Partner via C-CDAs and/or FHIR and USCDI. DOM expects to continue to receive data from DOM Trading Partners. There will be several different types of Trading Partners and the type and format may differ from one Trading Partner to the next. The Trading Partners include:

   a. Three Coordinated Care Organizations

   b. University of Mississippi Medical Center (Provider Trading Partner)

   c. Hattiesburg Clinic and Forrest General Hospital (Provider Trading Partner)

   d. Baptist Healthcare (Provider Trading Partner)

   e. Singing River Health System (Provider Trading Partner)

9. DOM requests that the Vendor provide a cost for new connections for Provider Trading Partners and Payers under Optional Services in Section VIII, *Cost Information Submission* of the RFP. This cost must cover all connection related activities as well as any membership fees that may exist. Membership fees can be priced as a pass-through cost to the agency.

10. Potential Provider Trading Partners and Payer types include HIEs – Health Information Exchanges.

11. DOM anticipates connecting to two emerging HIEs in Mississippi. These HIEs are the Hospital Association HIE, known as IntelliTrue and the Medical Association HIE, known as the Mississippi Health Access Exchange (MHAX).

   a. Vendor: Care Continuity (Hospital Association)

      Type of file: FHIR, USCDI, HL7

      Direction of data connectivity: Bidirectional.

   b. Vendor: KONZA, Inc. (Medical Association)

      Type of file: FHIR, USCDI, HL7

      Direction of data connectivity: Bidirectional.

12. Medicaid Provider's Electronic Health Record systems

13. Additional data from CCOs.

   a. Vendor must provide the ability to receive raw claims data from CCO's to facilitate the ability for DOM to analyze the original claim sent to the CCO from providers.

      Type of file: FHIR, USCDI, HL7 (or other)

      Size of current data source: approximately 27,000,000 claims annually

      Direction of data connectivity: Receive only.

   b. Medicaid Trading Partners, such as providers, CCOs, and third parties with clinical integrations, are asked to send to DOM only data on Medicaid Beneficiaries.

   c. Vendor must work with the new DOM EMPI vendor to accurately identify and separate inbound clinical data that belongs to a non-Medicaid Beneficiary. This

data must be routed to a repository that is separate from the generally accessible portion of the EDL. Data in this separate repository must be secured, encrypted, and retained by the IDA Vendor for seven years to comply with HIPAA requirements regarding retention of clinical data.

d. Vendor must report to DOM on a monthly basis the number of new records added to this repository, the number of existing records in the repository, and the number of records purged from the repository. These reports will contain no identifying information on the individuals whose data is in the repository and will be provided no later than ten business days after the month.

e. Vendor must complete an assessment with each DOM Trading Partner (currently, there are eight connected trading partners: five health systems and three CCOs) prior to go-live. The assessment must:

   1. Include a proposed method for transmitting data to DOM for data quality and potential improvements.
   2. Include a roadmap for continuous improvement in the C-CDAs, as well as FHIR/United States Core Data for Interoperability standards (USCDI), and HL7.
   3. Be completed annually for each connected Trading Partner.

f. Vendor must analyze sample C-CDAs, HL7, and FHIR/USCDI data provided by the State and Trading Partners to ensure that they understand the differences between these Trading Partners, data formats, and the requirements these differences may place on the Vendor's systems.

g. Vendor must document this analysis and discuss the results with DOM.

h. Vendor must determine and document an appropriate course of action to allow for these differences.

i. The proposed solution must ensure the successful intake of all files and message traffic in an appropriate amount of time, typically within one hour.

j. Vendor must report daily the total number of transactions received, successfully processed, and unsuccessfully processed by type and trading partner.

52. DOM EDL Control and Management tools:

   a. Data Traceability: All data loaded to the DOM EDL must be traceable back to its source. Information such as data source and date-time data loaded must be added to all records imported to the DOM EDL.

   b. Data Load reporting and error reporting: Reports on data loaded to the DOM EDL, and any data that fails to load to the DOM EDL must be available and actions must be available to resolve any load errors.

   c. Audit and Quality Control tools: Strong audit and quality controls must be built into the core of the DOM EDL.

53. Exchanging Data with DOM Trading Partners:

   a. The proposed solution must share administrative and clinical data with external Trading Partners including CCOs, HIEs, providers, and state agencies.

b. The proposed solution must authenticate and connect through the current Gainwell ESB. Inbound data from Trading Partners will pass through the Gainwell ESB which will pass the data to the EDL. Outbound data from the EDL will be passed to the Gainwell ESB for transmission to Trading Partners. It is DOM's vision that in the future, DOM will procure a new ESB, as a component of the new DOM Integration Layer, and thereby replace the existing DOM Interoperability Platform (ESB). The proposed solution must migrate from the existing DOM Interoperability Platform (ESB) and integrate with the new DOM Integration Layer, including using the Integration Layer's ESB component, Identity Management and Authentication Component, and FHIR services, using an interface as specified in this RFP, at no additional cost.

c. The proposed solution must integrate with the new EMPI to ensure that identities are matched correctly when data comes into the EDL from Trading Partners.

d. Vendor must work closely with the Gainwell ESB team and the new EMPI Vendor to ensure secure and reliable interaction between the EDL and these two components. Occasional improvements, updates, and maintenance of the Gainwell ESB and the new EMPI will require resources from the Vendor to accommodate and test the changes.

e. Vendor must provide documentation on their use of industry standard solutions for connectivity and security for all transactions between the EDL and the Gainwell ESB or the new EMPI.

f. Vendor proposal must include pricing for the following external connections:

1. Seven initial bi-directional connections to external Trading Partners using FHIR and USCDI for the exchange of clinical summaries with pricing for additional Trading Partners using these technologies. Pricing will include options for real-time or nightly batch for each connection.

2. Pricing for two initial bi-directional connections for HL7 Admission, Discharge, and Transfer (ADT) using RESTful web services with pricing for additional Trading Partners using these technologies. Pricing will include options for real-time or nightly batch for each connection.

3. Pricing for two initial bi-directional connections for C-CDA clinical summary using PDQ queries, XDS.b responses, and XDR push with pricing for additional Trading Partners using these technologies. C-CDA connectivity will be real time and will not include options for nightly batch.

4. The connections above may use technologies such as FHIR and USCDI that are used to fulfill the requirements of the CMS and ONC Final Rules on APIs, but the connections above are to be provided in addition to the Final Rule APIs. The Final Rule APIs are not included in the connections detailed in this section.

54. Accessing the DOM EDL:

a. Vendor must develop an EDL Gateway module that contains standard methods (APIs) for all access to data within the DOM EDL.

b. All access to data in the DOM EDL will be via the existing IOP Gateway provided by Gainwell. The only exception will be for audit and maintenance purposes.

1. The EDL Gateway must include referencing user roles to determine whether specific data should be returned as a result of the query.
2. The EDL Gateway must include cross referencing to the Beneficiary Opt Out data to determine whether specific beneficiaries' data should be returned as a result of the query. Whether or not data is returned will also depend on who is executing the query.
3. The EDL Gateway must include cross referencing to the Sensitive code processes to determine whether specific data held within the DOM EDL should be returned as a result of the query.
4. The EDL Gateway must include cross referencing to the HLI processes to include Standard Language for various code descriptions.

c. Vendor must implement multiple user roles to control who has access to data within the DOM EDL and what data the user may access.

d. The proposed solution must suppress the sending of data for all beneficiaries who chose to Opt Out of having their data shared. DOM will provide a weekly updated file containing a list of beneficiaries who have opted out.

e. Sensitive Codes:

1. Vendor must implement and support an integrated sensitive code solution that will integrate with all components of the Vendor's proposed IDA solution.
2. The sensitive code solution must contain a subset of diagnostic, procedural, and pharmacy codes that have been deemed sensitive by Federal and State law, and DOM policy.
3. Vendor must ensure all code sets are reviewed for sensitivity using the Federally mandated and State determined sensitive categories. Currently these are: Alcohol and Substance abuse, Sexually Transmitted diseases (STD's), and Mental Health (including intellectual and developmentally delayed).
4. Review of new or updated code sets must be completed within 20 business days of the date the code changes are published.
5. Should a new code set be published (i.e., ICD-11), the Vendor must ensure all codes within the code set are reviewed for sensitivity based on Federal and State law, and DOM policy.
6. The proposed solution must limit access to sensitive information based on the role of the user. There will be a need for multiple roles, and roles will be defined and approved by DOM.
7. The proposed solution must allow the export of a sensitive code set or subset to an Excel spreadsheet for publication to DOM providers or beneficiaries if requested.
8. Vendor must provide a user interface into the sensitive code solution to allow DOM staff to flag or remove a code as sensitive.

f. Health Language (HL):

1. Vendor must implement and support an integrated HL solution that will integrate with all components of the Vendor's proposed IDA Solution.

2. The HL solution must resolve all types of codes to their Natural Language description.

3. The HL solution must provide cross referencing between different coding systems. Current crosswalks include:

   a. CPT to CVX
   b. FDB to RxNorm
   c. FDB Allery to SNOMED
   d. HCPCS to NDC
   e. ICD9 to SNOMED
   f. CPT to LOINC
   g. CPT to SNOMED CT
   h. ICD-9-CM to ICD-10-CM
   i. ICD-9-CM to SNOMED CT
   j. CPT to CVX
   k. FDB to RxNorm
   l. SNOMED CT to CPT
   m. SNOMED CT to ICD-9-CM
   n. ICD-10=CM to SNOMED CT
   o. ICD-9-CM Procedures to SNOMED CT
   p. EPIC LAB to LOINC

g. Security and Access control:

1. The proposed solution must provide a single sign-on user access management function that allows users to access all components of the proposed solution. The IDA Vendor will be responsible for administration and management of all user roles.

2. The proposed solution must track and make available to DOM, all access to PHI and provide audit data related to the access. At a minimum, this shall include timestamp, content accessed, person that accessed, physical location of access with IP address, and method of access. This PHI access data will be kept permanently.

3. Data must be available to Trading Partners, DOM staff, auditors, and HIPAA reporting/auditing requests.

4. The proposed solution must prohibit unauthorized access to PHI and other sensitive information according to State and Federal confidentiality rules.

5. DOM currently supports federated identity via Azure Active Directory (AAD) across the Enterprise to allow secure end-to-end authentication for digital workloads. Proposed solutions must be able to federate with MDOM's identity and access management service (AAD). Both OAuth 2.0 and SAML are supported.

6. Vendor must follow Industry Standards and Best Practices for Software Development Life Cycle (SDLC) procedures.

7. The proposed solution must limit access to PHI and sensitive data based on the DOM user roles defined below:

a. Administrator
b. Super User
c. User with sensitive code access
d. User without sensitive code access
e. Trading Partner roles
f. API Vendor access user roles
g. Others as required

h. The proposed solution must support millions of real-time messages, such as HL7 ADT, per hour, each day (24 x 7). It must be able to respond to batch records requests, as well as real-time records requests. The solution must work seamlessly with the new Verato EMPI component, via a connection to the DOM Interoperability Platform (ESB), to first validate that the request is in fact for an active Medicaid beneficiary and responding with the appropriate data response.

i. The proposed solution, in cooperation with the new Verato EMPI component for identity verification, must validate requests for data, and then process, at a minimum, the records requests listed below, 24 hours per day 7 days per week:

1. 2,000 Patient Access real-time request/respond to patient record transactions per day
2. 3,000 Provider Information search requests per day
3. 3 million real-time ADT records batch load per day
4. 500,000 real-time and batch requests for other types of transactions per day
5. Support adequate data analytics/reporting and Machine Learning process

55. Interaction with other DOM Applications:

a. The proposed solution must integrate with the new EMPI from Verato and use it to resolve beneficiary identities both when loading data to the EDL and when responding to requests for beneficiary data from the EDL.

b. All components of the new IDA solution must integrate with the ESB, as the connectivity and interoperability broker, and work with the Vendor, Gainwell Technologies LLC, for integration and operations, including technical support coordination. All components will be required to be migrated to integrate with the new DOM Integration Layer, as a replacement to the existing DOM Interoperability Platform (ESB), using an interface as specified in this RFP, at no additional cost, when such tools are procured in the near future, including a new ESB service and Identity Management and Authentication Services.

c. The proposed solution must have the capability of obtaining a DOM Enterprise Unique Identification (EUID) from the EMPI before loading the record into the EDL.

d. The EUID is managed and subject to change by the EMPI.

e. Vendor must supply supplementary matching data where available. For example, beneficiary identity data such as the Trading Partner's Member Record Number (MRN) will likely be received in incoming data. This MRN information will be added to the EMPI as an alternate identity to assist with future matching.

56. LTSS

a. DOM is currently transitioning Electronic Long-Term Services and Support (eLTSS) and Electronic Visit Verification (eVV) services. The IDA Vendor will be required to integrate LTSS and eVV to the IDA Solution using an interface as specified in this RFP, at no additional cost.

C. Patient, Payer, and Provider Directory APIs

Vendors must provide pricing for the following APIs as a separate, optional component of the RFP response. Vendors must describe in detail how it plans to meet each of the following API requirements.

57. The proposed solution must provide a Patient Access API, Payer-to-Payer API, and Provider Directory API compliant with 2020 Final Rules on APIs from CMS and the ONC (CMS 9115-F). These APIs will allow Medicaid beneficiaries and payers to retrieve data from DOM in an automated fashion using technologies that include FHIR and the USCDI. The CMS Final Rule and requirements for Medicaid and CHIP plans can be found at the Federal Register, 45 Code of Federal Regulations (CFR) Part 156 (CMS – 9115-F): https://www.govinfo.gov/content/pkg/FR-2020-05-01/pdf/2020-05050.pdf

58. CMS has issued API implementation guides. DOM expects Vendors to follow the recommendations of CMS guides unless DOM and the Vendor agree otherwise. The guides can be found here:

    https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index

59. The ONC Final Rule and requirements for developing FHIR APIs and USCDI as a data format can be found at the Federal Register, 45 CFR Parts 170 and 171 (RIN 0955 – AA01):

    https://www.govinfo.gov/content/pkg/FR-2020-05-01/pdf/2020-07419.pdf

60. Vendor must develop all three APIs in compliance with the CMS Final Rule, the ONC Final Rule, and the CMS API implementation guides. Further details on the APIs:

    a. Patient Access API: A Medicaid and CHIP Patient Access API which uses FHIR and USCDI. Vendor must develop, document, and support an API using a standards-based FHIR interface to support the automated requests and responses from Medicaid and CHIP beneficiaries for their clinical and claims-based data in the USCDI format. Neither the Vendor nor DOM are required to provide the software that beneficiaries use to request and view their data. The Vendor must integrate this and all other APIs with the DOM EDL and will not rely on a separate, dedicated data repository. The Vendor must integrate this API with the DOM Interoperability Platform (ESB) or any replacement thereof, using an interface as specified in this RFP, at no additional cost.

    b. Provider Directory API and Website: A Provider Directory which shall be published and maintained for all Medicaid providers on the DOM website, along with a Provider Directory API. The Vendor must develop, document, and support a list of providers on a website as well as develop a FHIR API to share Provider Directory data. This Provider Directory data must be accessible by Medicaid beneficiaries and other stakeholders without special effort on devices such as phones, tablets, and computers. Vendor will use Provider Directory data elements specified in the Final Rule and include elements such as provider

name, address, and hours of care. This API must be integrated with the DOM Interoperability Platform (ESB) or any replacement thereof, using an interface as specified in this RFP, at no additional cost. The Provider Directory API shall be compliant with supporting the exchange of Prior Authorization data, as required in the CMS proposed Final Rule of December 2020.

c. Payer to Payer API: A Medicaid and CHIP Payer to Payer API which uses FHIR and USCDI. The Vendor must develop, document, and support a standards-based FHIR API to support the requests and responses from payers for clinical and claims-based data on beneficiaries in the USCDI format. The API created by the Vendor will be serviced by the DOM EDL and will not rely on a separate, dedicated data repository. This API will be integrated with the DOM Interoperability Platform (ESB) or any replacement thereof, using an interface as specified in this RFP, at no additional cost. All existing CCOs and Trading Partners currently connected to the DOM Interoperability Platform (ESB) shall be converted from the current RESTful Web Service interface to the Payer API and migrated from C-CDA data exchange to support USCDI over FHIR (or other acceptable data formats, such as claim formats, etc., over FHIR).

61. API Data Sources:

  a. In order to fulfill the goal of providing Medicaid beneficiaries and payers complete data from DOM in an automated fashion, the Vendor solution must provide data to the APIs sourced from the DOM EDL. The APIs must not be served by a dedicated database separate from the EDL.

  b. All data exchanged with parties outside DOM must go through the DOM Interoperability Platform (ESB) or any replacement thereof. Each API must build the connection interface to the DOM Interoperability Platform (ESB) or any replacement thereof.

  c. Authentication and Authorization: The DOM Interoperability Platform will be responsible for the secure connection to all outside applications using OAuth 2.0. Outside sources include:

    1. Patient Access API: API will authenticate the request based on DOM beneficiary information.
    2. Payer to Payer API: API will authenticate the request based on preset DOM partner information.
    3. Provider Directory API: As provider information is public, Provider Directory API has no need for authentication.

  d. The three types of API requests will originate from consumer websites, services, smartphone apps, and devices over FHIR using the to-be-developed DOM FHIR APIs.

  e. External API requests will pass to the existing DOM Interoperability Platform which will then send requests to the DOM EDL. At the DOM EDL, the request will be authenticated and, if authorized and appropriate, a response will be generated in real-time back to the DOM Interoperability Platform with appropriate data to fulfill the request in the correct format.

    f. Authentication will use OAuth 2.0 and employ criteria including whether the request is for an appropriate Medicaid or CHIP beneficiary identity and whether the request originates from an authorized user.

    g. Vendor will be responsible for developing the three APIs outlined above, connecting the three APIs to the DOM Interoperability Platform, and supporting the bi-directional requests and responses to the patient, the payer, or another party via the public facing FHIR APIs connected to the DOM Interoperability Platform. Each of the three APIs must have the capacity to support a minimum of 500 API requests per hour.

62. API Operations Support and Maintenance

    a. Vendor must perform all maintenance and operational support of the solution.

    b. Vendor must maintain and update the FHIR API interfaces, keeping them in sync with new versions of FHIR and data in the DOM IDA Project.

    c. Vendor is not required to provide support to end users of the Patient Access, Provider Directory, and Payer APIs. However, DOM may request changes and improvements to Vendor's APIs and documentation based on complaints or suggestions from API users.

    d. Vendor must maintain clear documentation on the APIs which DOM will post on the DOM website. Documentation must clearly define how to develop and maintain applications and services that work with the APIs and be reviewed and updated every 30 days per the CMS Final Rule (CMS 9115-F).

    e. Vendor must create and maintain no more than five "handout" or "flier" documents intended for end users. No such handout will be needed for the payer-to payer API as the consumers of that API will be other payers who have dedicated IT staff. These documents will:

        1. Be distributed by DOM resources during beneficiary enrollment and outreach activities.

        2. Include non-technical information on the patient and provider directory APIs.

        3. Describe the information available from the APIs and describe in general how a user may obtain an application that can make API requests and display the resulting data.

        4. Note that neither DOM nor the Vendor is responsible for providing or supporting applications that use the APIs.

63. API Requirements

    a. Vendor must provide the following elements for API development based on the FHIR structure as outlined by HL7 standards. Note that the HL7 website below and CMS implementation guides have the authoritative requirements, and the details below are provided only as a summary. The HL7 FHIR standard may be found here:

    https://www.hl7.org/fhir/modules.html

    b. Level One:

        1. Foundation: The basic definitional infrastructure on which the rest of the specification is built.

a. Base Documentation, XML, JavaScript Object Notation (JSON), Data Types, Extensions.

c. Level Two:

1. Implementer Support: Services to help implementers make use of the specification.

   a. Downloads, Version Management, Use Cases, Testing.

2. Security & Privacy: Documentation and services to create and maintain security, integrity, and privacy.

   a. Security, Consent, Provenance, Audit Events.

3. Conformance: How to test conformance to the specification and define implementation guides.

   a. Structure Definition, Capability Statement, Implementation Guide, Profiling.

4. Terminology: Use and support of terminologies and related artifacts.

   a. Code System, Value Set, Concept Map, Terminology Services.

5. Exchange: Defined methods of exchange for resources

   a. Rest API + Search, Documents, Messaging Services, Databases.

d. Level Three:

1. Administration: Basic resources for tracking.

   a. Patient, Practitioner, Care Team, Device, Organizations, Location, Healthcare Services.

e. Level Four:

1. Clinical: Core clinical content.

   a. Allergy, Problem, Procedure, Care Plan/Goal, Service Request, Family History, Risk Assessment, etc.

2. Diagnostics: Ordering and reporting of clinical diagnosis.

   a. Observation, Diagnostic Report, Service Request, Media, Specimen, Imaging Study, Genomics, etc.

3. Medications: Medication management and immunization tracking.

   a. Medication, Request, Dispense, Administration, Statement, Immunization, etc.

4. Workflow: Managing the process of care, and technical artifacts to do with obligation management.

   a. Introduction + Task, Appointment, Schedule, Referral, Plan Definition, etc.

5. Financial: Billing and Claiming support.

   a. Claim, Account, Invoice, Charge Item, Coverage & Eligibility, Request & Response, Explanation of Benefits, etc.

f. Level Five:

1. Clinical Reasoning: Clinical Decision Support and Quality Measures.

   a. Library, Plan Definition and Guidance Response, Measure/ Measure Report, etc.

64. Vendor must provide the following documentation and deliverables for the API solution.

    a. Phase 1 - Business Discovery Documentation

        1. Solution Design

    b. Phase 2 - Technical Design Documentation

        1. Hosting Infrastructure

           a. High Availability

           b. Disaster Recovery

        2. Application Architecture

           a. Workflow

           b. FHIR interfaces to DOM Interoperability Platform (ESB)

           c. Error handling, alert, and recovering logic

        3. FHIR module design

        4. USCDI data repository, data request validation logic, and data mapping logic

        5. Beneficiary record view/access strategy

    c. Phase 3 - Development and Configuration that includes a development, user acceptance, and production environment for the APIs below and the data repository with supporting validation and logic.

        1. Medicaid and CHIP Patient Access API

        2. Provider Directory and Provider Directory API

           a. Design and implement a provider repository with single best record view

           b. Develop Provider Directory data collection and maintenance processes

           c. Develop Provider Directory Access Portal that is humancentric

        3. Medicaid and CHIP Payer to Payer API

        4. USCDI data repository and all associated interfaces, business and validation logic, and data mapping to the USCDI format

    d. Phase 4 - Testing that will be conducted through all environments for each of the items below.

        1. Medicaid and CHIP Patient Access API

        2. Provider Directory and Provider Directory API

        3. Medicaid and CHIP Payer to Payer API

        4. USCDI data repository and all associated interfaces, business and validation logic, and data mapping to the USCDI format

    e. Phase 5 - Deployment that will be conducted through the environments for each of the items below.

        1. Medicaid and CHIP Patient Access API

        2. Provider Directory and Provider Directory API

        3. Medicaid and CHIP Payer to Payer API

    4. USCDI data repository and all associated interfaces, business and validation logic, and data mapping to the USCDI format

  f. Phase 6 - Maintenance and Operations of all environments to accurately test and deploy new development as it is released

D. Standards

Vendor must describe in detail how it plans to meet each of the following requirements.

65. The IDA Solution must support common healthcare terminology standards that include but are not limited to Unified Code for Units of Measure (UCUM), Systematized Nomenclature of Medicine – Clinical terms (SNOMED CT), RxNorm, RadLex, MEDCIN, International Classification of Diseases, Tenth Revision (ICD-10), Healthcare Common Procedure Coding System (HCPCS), Manufacturers of Vaccine (MVX), National Drug Codes (NDC), and Logical Observation Identifiers Names and Codes (LOINC).

66. The new Medications exchange standard must be HL7 FHIR v4.01 or higher and backward compatible with C-CDA v2 or higher and the standard for vocabulary used must be NCPDP (retail pharmacy), NDC, and RxNorm.

67. The new demographics exchange standard must be HL7 FHIR v4.01 or higher.

68. The new Problem/Symptom exchange standard must be HL7 FHIR v4.01 or higher and the standard for vocabulary used must be ICD-9-CM, ICD-10-CM, and SNOMED CT.

69. The new Procedures exchange standard must be HL7 FHIR v4.01 or higher and the standard for vocabulary used must be Current Procedural Terminology (CPT-4), Healthcare Common Procedure Coding System (HCPCS), and SNOMED Clinical Terms (SNOMED CT).

70. The new Allergies exchange standard must be HL7 FHIR v4.01 or higher and the standard for vocabulary used must be SNOMED CT, RxNorm, and NDC.

71. The new Hospital/Physician Visits exchange standard must be HL7 FHIR 4.01 or higher and the standard for vocabulary used must be ICD 9-CM, ICD-10 CM, CDT-4, and SNOMED.

72. The ADT exchange standard must be HL7 v2.5 ADT or higher. The IDA Solution must have standard user-based access control.

73. Vendor must support Health Information Trust Alliance (HITRUST), Federal Risk and Authorization Management Program (FedRAMP), as well as the ONC and CMS Final Rules.

74. The proposed solution must support the following healthcare interoperability standards:

  a. FHIR v4.01 or higher

  b. C-CDA v2 or higher

  c. HL7 2.5 or higher

  d. USCDI v2 or higher

75. The proposed solution must have a data processing logic module that should be de-coupled from the data storage to support DOM data exchange and Interoperability.

76. The proposed solution should adopt data integration best practices for data uploading, transformation, and synchronization. Vendor must describe the data integration tools they plan to use whether they are provided by the Vendor or a third party.

77. Vendor must comply with the requirement that all data exchanged with outside Trading Partners will go through the DOM Interoperability Platform (ESB) and any replacement thereof.

78. Awarded Vendor must follow the standards and best practices to provide the required inbound and outbound RESTful web service/FHIR adapters between EDL and DOM Interoperability Platform (ESB) and any replacement thereof.

79. The proposed solution must authorize and validate the request and respond in real-time back to the DOM Interoperability Platform (ESB).

80. The proposed solution must support both synchronous and asynchronous transactions

81. EDL's response to the beneficiary clinical data query from DOM Interoperability Platform (ESB)must be viewable, usable, and consumable by the device or consumer website/service without translation at the DOM Interoperability Platform (ESB)or at the consumer website/service or device.

82. EDL response to the beneficiary query for their clinical data must conform to the device or consumer website/consumer service per the device or consumer website/consumer service's implementation guide (i.e., Apple Health Record System).

83. Vendor must maintain and update both the FHIR interface (API) between the EDL and the DOM Interoperability Platform (ESB), keeping the FHIR interfaces (API) in synch with the DOM Interoperability FHIR interfaces (API).

84. Vendor must provide updates, fixes, patches, and future releases of FHIR as a standard, as well as comply with requirements from CMS in Final Rule (CMS 9115-F).

85. Vendor must perform all maintenance and operational support of the FHIR interfaces (API) and data sets for the IDA solution.

86. Vendor must coordinate the support tickets and tasks with other Vendors' support resources to support DOM users, the DOM Interoperability Platform, and other Vendors' Help Desks, as necessary. The Vendor must work with Vendors that support DOM services such as EMPI, MES, and Eligibility and Enrollment (E&E).

E. Hosting Requirements, (including operations and performance)

Vendor must describe in detail how it plans to meet each of the following requirements.

87. By default, all IDA systems should be hosted in a Cloud solution. Vendors must state in which cloud the solution will be hosted.

88. Vendor shall follow Industry Standards and Best Practices for hosting and security.

89. **MANDATORY:** Vendor shall be aware that under no circumstances shall any data, or equipment associated with this project reside outside the continental United States, nor shall any data, or equipment associated with this project be accessible

to people outside the continental United States. Vendor must describe how this requirement will be met.

90. The new IDA Solution must be implemented and operated in a SaaS model with full support of HL7 FHIR/USCDI. DOM will not be operationally responsible for any aspect of the solution.

91. Vendor must provide a disaster recovery (DR) Data Center location in the continental United States that is at least 500 miles from the primary facility. Vendor's proposal must describe how the DR Data Center location minimizes risk in the event of disaster, including service levels for recovery and minimizing data loss.

92. Vendor must provide network protection to prevent attacks on DOM's servers and data and to ensure DOM's data, information, and networks are secured to prevent unauthorized access.

93. Vendor must ensure the facility is compliant with Statement on Standards for Attestation Engagements (SSAE) No. 16 and HIPAA standards.

94. Vendor must provide the Data Center and hosting capacity to be scalable and extendable to support their component(s) and future growth over the duration of the contract at no additional cost to the State.

95. Vendor must provide all hardware and software required to provision, monitor, and manage the circuit to the hosting and DR facilities.

96. Vendor must demonstrate in the proposal its ability to increase the capacity of the circuit in incremental increases of 100 Mbps and one Gbps should DOM require an increase in the future. Pricing must be presented in the RFP Section VIII: *Cost Information Submission* as an optional cost.

97. Vendor must provide wide area network (WAN) encrypted tunnel or virtual private network (VPN) tunnel support to DOM from both the primary and the DR site.

98. Vendor must provide a firewall and security solution that complies with the transmission security provisions of HIPAA, as well as all relevant federal, state, and local laws.

99. Vendor must provide a description of the proposed network security and the effectiveness of the proposed system protocols and measures to prevent intrusion and protect DOM's data.

100. Vendor must provide security services that include the following:

    a. Monitoring for timely reporting of threats and intrusions.
    b. Security protections to prevent unauthorized access to DOM's information, software, and systems.
    c. Security agent to control all traffic between the primary and DR center and the outside world and protect against unauthorized access or intrusions.
    d. Allow reporting for firewall and other statistics from any Internet browser with monthly analysis and recommendations to improve security and throughput.
    e. Ensure the security, integrity, and availability of the data to DOM and must describe in its proposal the levels it will achieve and how the Vendor intends to achieve security, integrity, and availability, including DR services.

f.   System and data reliability through off-site system and data backup in accordance with the SLA.

g.   Record and report security incidents and breaches (both immediate and summary reporting).

h.   Perform reporting on login attempts.

i.   Managed services, including:

1.   Managed firewall,
2.   System and application monitoring,
3.   Performance monitoring,
4.   Server startup and shutdown support,
5.   Hardware maintenance,
6.   Network alerts,
7.   Troubleshooting and response,
8.   Operating system patch installation and minor upgrades,
9.   File system management support,
10. Failure tracking, and
11. Backup and restore of all system components and data.

j.   Vendor must submit a monthly report monitoring the status from the previous month.

k.   Vendor must implement and support a software version control application to maintain the compiled code.

l.   Vendor must provide Database Performance Reports upon request.

m. Vendor must maintain the TOP and provide updates annually or within 30 days of changes that impact backup, DR, or other continuity of operations activities.

101. Information Security Requirements:

a.   To ensure sufficient data protection safeguards are in place, Vendor and all Subcontractors must at a minimum implement and maintain the following at all times, at no additional cost to the State. The Vendor and/or Subcontractor may augment this list with additional information technology controls:

1.   Apply hardware and software hardening procedures as recommended by the manufacturer to reduce the components surface of vulnerability. These procedures may include, but are not limited to, removal of unnecessary software, disabling or removing of unnecessary services, removal of unnecessary usernames or logins, and deactivation of unneeded features in the components' configuration files.

2.   Establish policies and procedures to implement and maintain mechanisms for regular internal vulnerability testing of operating system, application, and network devices supporting the two components, EDL and CMS Final Rule APIs. The Vendors and/or Subcontractor must evaluate all identified vulnerabilities for potential adverse effect on the system's security and integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. DOM must have the right

to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided.

3. External vulnerability testing is an assessment designed to examine the Vendor's security profile from the Internet without the benefit of access to internal systems and networks behind the external security perimeter. Where website hosting or Internet access is included as part of the services provided under this RFP, the Vendors must conduct regular external vulnerability testing. The Vendor must evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effects on the system's security and integrity. The Vendor must remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. DOM must have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided.

4. Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the components services. Ensure that the anti-virus and anti-malware software is automatically updated. Ensure that the software is configured to actively scan and detect threats to the system for remediation.

5. Enforce strong user authentication and password control measures over the components to minimize the opportunity for unauthorized system access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with NIST 800-53 (Moderate Baseline) controls, including specific requirements for password length, complexity, history, and account lockout.

6. Ensure that DOM data is not being commingled with the Vendor's other clients' data. This includes, but is not limited to, classifying data elements and controlling access to those elements based on the classification and a user's access or security level.

7. Apply data encryption to protect DOM data from improper disclosure or alteration. Data encryption must be applied to DOM data in transit over networks, DOM data at rest within the system, and DOM data when archived for backup purposes. Encryption algorithms that are used for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2. https://csrc.nist.gov/publications/detail/fips/140/2/final

8. Enable appropriate logging parameters on systems supporting the components to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers.

9. Retain the logs and identify suspicious or questionable activity for investigation. Vendor must document the cause and perform any required remediation.

10. Ensure system and network environments are separate by properly configuring and updating firewalls to protect and isolate DOM data from unauthorized access.

11. Restrict network connections between trusted and untrusted, isolating systems supporting the components from unsolicited and unauthenticated network traffic.

b. Vendor must adhere to an industry standard (e.g., NIST 800-61) security incident response protocol and incorporate related actions into the Vendor's processes and procedures for coordinating information security incident handling with DOM.

F. Vendor Background, Experience, and Staffing Requirements

Vendor must describe in detail how it plans to meet each of the following requirements.

102. Corporate Experience

a. **MANDATORY:** Awarded Vendor must have a minimum of two years of healthcare information technology solution development, implementation, ongoing operations, support, and maintenance experience relevant to this procurement and should detail this experience in the proposal.

b. **MANDATORY:** Awarded Vendor must have a minimum of five years' experience in Medicaid healthcare IT (e.g., Medicaid claims processing (MMIS), eligibility and enrollment system, Medicaid HIT, etc.).

c. Vendor shall provide a description that contains all pertinent data relating to the Vendor's organization, personnel, and experience that would substantiate the qualifications and capabilities of the Vendor's company to perform the services described herein.

d. A brief history of the company including:

1. Date of establishment

2. Organization size (i.e., number of offices, employees, customer base, etc.) and structure

3. Whether the company is based locally, regionally, nationally, or internationally

4. Number of years the company has been in business (minimum of five years is required)

5. Type of company ownership (public or private) and type of organization (limited partnership, non-profit, etc.)

e. Corporate information to include parent corporation, sister firms, and any subsidiaries.

1. State of incorporation - The Vendor's firm shall be licensed to provide the proposed services in the State of Mississippi.

2. Location of Vendor's principal office and the number of executive and professional personnel employed at this office.

3. Current products and services/lines of business and approximate percentages.

4. Disclosure of any company restructurings, mergers, and acquisitions in the past three years or planned in the upcoming 18 months that will have impacted or may impact any products the Vendor sells, services, and supported.

5. For any Vendor parent, affiliate, or subsidiary organization, Vendor shall provide to DOM written authorization from the Vendor's parent, affiliate, or subsidiary's authorized representative for DOM to access Vendor's parent, affiliate, or subsidiary organization's records where such a relationship exists that would impact Vendor's performance under the contract.

6. The Vendor shall provide information on any professional accreditations/certifications pertinent to the services required by this RFP.

7. Financial information as follows:

   a. The State reserves the right to request information relative to a vendor's references and financial status and to visit a Vendor's facilities during normal working hours.

   b. The State reserves the right to request a current financial statement, prepared and certified by an independent auditing firm, and reserves the right to require that Vendors document their financial ability to provide the products and services proposed up to the total dollar amount of the Vendor's cost proposal.

   c. The State, at its sole discretion, may reject the proposal of a Vendor with any significant outstanding financial or other obligations to the State or who is in bankruptcy at the time of proposal.

103. Vendor IDA Key Team Members:

   a. Project Sponsor

      1. Vendor must describe the proposed personnel and submit a resume.
      2. For the duration of the project, the IDA Vendor must provide an overall Project Sponsor with onsite responsibilities at the Vendor provided office facility once per month for the DOM monthly Steering Group meetings.

   b. Project Manager

      1. Vendor must describe the proposed personnel and submit a resume.
      2. For the duration of the project, the IDA Vendor must provide a Project Account Manager with onsite responsibilities at the Vendor provided office facility for a minimum of 80 hours per month.

   c. Lead Project Manager

      1. Vendor must describe the proposed personnel and submit a resume.
      2. Perform overall project planning (including a detailed project plan in Microsoft Project), project reporting, project management, quality assurance, and documentation as needed or required by DOM.
      3. Manage the overall project in accordance with the project plan.
      4. Create monthly overall status report.

5. Manage Vendor team members including the IDA Vendor Technical Architect, Business Analyst's (BA), QA Lead, and all staff to support the solution for the duration of the contract.

6. Create and maintain Risk and Issue Registers.

7. Support the work of the IV&V Vendor with testing, including User Acceptance Test (UAT) and validating performance, stress testing, and other testing and validation as deemed necessary.

8. Report to the DOM IDA Project Manager and serve as liaison to the IV&V.

9. Perform responsibilities onsite for a minimum of three weeks per month from project initiation until completion of project go-live.

10. Onsite responsibilities post go-live one week per month for duration on the contract.

11. Attend Monthly Steering Group Meeting onsite at DOM in Jackson, Mississippi and present overall status, issues, and risks to participants.

12. PMP certification is preferred for this role.

d. Technical Architect

1. Vendor must describe the proposed personnel and submit a resume.

2. Minimum five years of experience with healthcare information technology projects, including two years of experience with Medicaid and/or clinical data and two years of experience with healthcare interoperability.

3. Minimum three years of experience with design and implementation of large data integration platform, be proficient in data architecture design and data integration with data virtualization technology, and be familiar with DB design, performance tuning, and Extract, Transform, Load (ETL) processes.

4. Lead technical planning and design of the solution, including integration of the solution with the existing DOM EMPI for seamless data exchange in real-time.

5. Provide overall technical Subject Matter Expertise.

6. Perform responsibilities onsite at the Vendor provided office facility for a minimum of 80 hours per month from project initiation until completion of project go-live.

7. Provide onsite support and resources during all testing for the duration of contract.

e. Database Administrator (DBA)

1. Vendor must describe the proposed personnel and submit a resume.

2. The DBA must have at a minimum, five years of experience with data lake/ data warehouse design, including two years of experience with healthcare data management.

3. Must understand common challenges and corresponding solutions that accompany a data lake implementation, and be familiar with database performance tuning, and Extract, Transform, Load (ETL) processes.

4. Must be an expertise in SQL and NoSQL design and familiar with Data Virtualization and master data management.

    5. Provide overall technical Subject Matter Expertise, and support for implementation and operation.

f. Clinical Business Analyst

    1. Vendor must describe the proposed personnel and submit a resume.

    2. Must be a healthcare professional with a preference for a Registered Nurse or equivalent with a minimum of five years' experience in a clinical healthcare setting with EHR experience. This resource must possess strong knowledge in all aspects of patient care and clinical workflows, technical expertise to include strong understanding of business requirements development, in addition to providing clinical support that will meet the clinical requirements of the overall solution.

    3. Provide overall Clinical Subject Matter Expertise, including assisting the IDA Vendor with testing and QA of the product and product updates to ensure clinical compliance and clinical integrity of the solution, such as validation that clinical data is displaying properly, non-duplicative clinical data is available or being displayed, correct clinical data is being processed, stored, and displayed, and the solution is correct and usable by clinical staff.

    4. Assist the DOM team with user acceptance testing (UAT) of the solution for clinical compliance, such as with any changes, updates, patches, or fixes as necessary and requested by DOM.

    5. Perform responsibilities onsite at the Vendor provided office facility or a minimum of 80 hours per month from project initiation until completion of project go-live.

    6. Provide onsite support and resources during all testing (for DDI and then after go-live) including supporting the DOM team in testing updates, patches, fixes, and upgrades, for the duration of contract.

g. QA Team Lead

    1. Vendor must describe the proposed personnel and submit a resume.

    2. Manage the processes and personnel to conduct quality assurance testing, conduct rigorous testing throughout the development process, identifying potential issues, and reporting them back to development teams and DOM project manager.

    3. Must have a minimum three years of experience with leading healthcare data QA. In-depth knowledge of data handling and transformation techniques such as ETL, Test Data, and Test Environment management concepts, tools, and practices. Strong managerial, analytical, and critical thinking.

h. Ongoing Training and Adoption Staff

    1. Provide staff training for adoption, utilization, and best practices to multiple DOM and State staff. Provide onsite (Jackson, Mississippi) resource(s) twice a month (eight business days) during the first year of operations of the component, moving to one week a month (five business days) thereafter.

i. Project Staffing

    1. Awarded Vendor must provide a team of personnel to support each component's initiation, design, development, and implementation including

any necessary integration with Trading Partners, testing, go-live, warranty period, and ongoing operations, support, and maintenance.

2. Any proposed team must include resumes with the RFP response of key team members with experience highlighted on similar projects.

3. Vendor must submit with their proposal a detailed staffing plan that provides details including allocations and onsite commitments by resource for their proposed team.

4. Key team members are mandatory and must be onsite in Jackson, Mississippi regularly, including during UAT. The awarded Vendor must provide office space, equipment, and lifecycle management tools as necessary for this team, including access for DOM. There is limited office space for this team at DOM. Vendor should use their experience to provide details in their proposal as to which Key Team members will be onsite and for what percentage of time during the project.

5. Key team members proposed as part of the solution will remain on the project team for the duration of the project unless a change in the team is the result of a request or approval by DOM. The Vendor must provide a staffing contingency plan for all key personnel, which must be updated annually, at a minimum.

6. Vendor must provide onsite Subject Matter Experts (SME), BAs, and other staff as needed for the IDA Project.

7. The SMEs/BAs must have a minimum five years of experience with healthcare technology projects including two years of experience with Medicaid and/or clinical data.

8. Vendor must provide technical training onsite for the solution, the workflows, and audit logs for up to five Administrators.

9. Vendor must provide detailed training documentation and system documentation via technical solution and component specifications. All documentation must be updated on a regular basis, with updates occurring every six months at a minimum.

j. Project Management Requirements

1. Vendor must create and maintain a dedicated DOM-specific, secure document repository accessible by the Vendor, DOM, IV&V, and other parties as the needs of the agency change. The Vendor must describe the repository product and methodology in detail.

2. Vendor must follow industry standard, best practices (Certification Commission for Health Information Technology (CCHIT), Practice Management Institute (PMI), and Project Management Body of Knowledge (PMBOK)), and the specific project management processes implemented by the DOM Office of Information Technology Management (iTECH). These processes do not dictate how the project must be managed but will require some standard deliverables.

3. Vendor must provide a detailed Business Requirements document and Requirements Traceability Matrix (RTM) developed collaboratively by the Vendor and the DOM Team. These detailed business requirements and descriptions must be reviewed and approved by DOM prior to the beginning of development or configuration tasks.

4. Vendor must provide a detailed Test Management Plan that addresses test approach and methodology. The Test Management Plan includes, but is not limited to, development of test cases, test case traceability and testing tools, test execution, defect resolution, and test reporting for all phases of testing.

5. Vendor test cases must be cross walked to each identified business requirement, technical design, and healthcare IT industry standard.

6. Vendor must provide a Training Plan. The Vendor will be responsible for training DOM staff onsite in Jackson, Mississippi, who will then train other DOM staff (Train the Trainer).

G. Vendor and Project Management Requirements

104. Vendor must fully document all aspects of the solution and will, throughout the life of the contract, maintain and deliver to DOM all documentation to reflect the current state of the application(s) and update all documents annually at a minimum, unless otherwise stated in this RFP. All documentation will be available to DOM via an electronic document repository provided by the Vendor and will remain with DOM until the end of the contract period at no additional cost.

105. Vendor must deliver initial training documentation to DOM for review and approval 30 days prior to UAT start.

106. Vendor must deliver final updated Technical Architecture Design documentation, including a high-level data flow diagram and a technical diagram of the entire solution, to DOM for review and approval 30 days post go-live.

107. Vendor must submit a baseline Business Continuity and Disaster Recovery (BC-DR) Plan for approval by DOM.

   a. The BC-DR Plan will be reviewed and updated at least once per year.

   b. Vendor must communicate proposed modifications to the BC-DR Plan at least 30 calendar days prior to the proposed incorporation for DOM's review and comment.

   c. An outline of the key aspects of the Vendor's approach to DR must be submitted with Vendor's proposal.

108. The State utilizes infrastructure health monitoring tools that track network and application performance and health. Application Monitoring Tools (APM) are utilized to gather and quantify Enterprise performance. The APMs are expected to monitor systems such as the hosting platform, process utilization, memory demands, process duration, and disk read/write speeds.

109. The intent is to install software agents on Vendor's system(s) providing independent visibility into performance. The information provided can augment, support, or potentially act in lieu of Vendor specific SLA reporting. DOM uses infrastructure monitoring to quickly identify breakdowns in systems that are considered critical data provider resources in a multi-vendor enterprise.

   a. Vendor must provide a mechanism for DOM to ingest performance data via an industry standard mechanism such as Open Telemetry that is sufficient for monitoring SLA compliance.

   b. Vendor shall provide State agents access to technical resources capable of supporting APM tool in the networking and application infrastructure.

    c. Vendor shall partner with the State to resolve issues when an APM tool provides feedback indicating issues exist with the vendors infrastructure that are impacting the system or related components.

H. Operations, Support, and Maintenance

110. Federal, State, and DOM Requirements

    a. Vendor must follow a standard escalation procedure and develop an operations best practice guide to ensure that the Vendor:

1. Detects, identifies, and reports system problems as they occur.
2. Detects and reports PHI data breaches within 24 hours of occurrence.
3. Escalates problems within 30 minutes of initial Help Desk contact.
4. Communicates to end-user/customer administrators within one hour of initial escalation.
5. Contacts end-user/customer administrators with resolution/preventative action taken within eight hours.

111. Change and Testing Management

    a. Vendor must document and follow a rigorous Change/Configuration Management process to include the following:

1. Methodology and approach to control project artifacts and system functionality changes.
2. Change management and version control tool(s) and supporting procedures.
3. Release management tool(s) and supporting procedures.
4. Change/Configuration Management roles and responsibilities.
5. Methodology and approach to ensure validation of all components, data, and related integrations, including appropriateness of test methods and testing tools throughout all phases of testing.
6. Test cases along with corresponding test results that provide full coverage of traceability to both business and technical requirements.
7. Defect management including recording, tracking, resolution, reporting activities, and tools.
8. Use of DOM-relevant data for testing, including converted data.
9. Testing management roles and responsibilities including QA manager, QA Architect, and QA testers.
10. Testing metrics and reporting throughout all phases of testing.
11. Unit testing to ensure changes meet technical specifications including evidence that demonstrates successful unit test results as required.
12. QA testing to ensure system components and a collection of integrated components function as designed.
13. QA test results must be delivered to and reviewed by DOM for approval prior to entering UAT.
14. Regression testing throughout all phases of testing as applicable to ensure full coverage of validation for all system components.

15. Regression test results must be delivered to and reviewed by DOM for approval prior to entering UAT.

16. Performance/Stress testing to ensure all IDA components and Data Integrations meet established performance metrics.

17. Performance/Stress test cases and results must be delivered to DOM as required.

112. Quality Management and Quality Review

   a. Vendor must develop a Quality Management Plan that covers all phases and functions of the project.

   b. Vendor must perform quality reviews, QA, and quality control audits throughout the duration of the project.

   c. Vendor must employ an internal quality assurance and quality control process to ensure that all deliverables, documents, and calculations are complete, accurate, easy to understand, and of high quality. Quality activities include but are not limited to:

      1. Ensuring a Deliverable Expectation Document (DED) is developed and approved by DOM that defines deliverable requirements and expectations.

      2. Ensuring all deliverables are adhering to established standards (order and formatting), are responsive to the specific requirements (for example, comparing the deliverable against the deliverable expectation document), and contain no spelling or grammatical errors via internal quality review processes prior to distribution to DOM/stakeholders.

      3. Ensuring required tasks, timelines, meetings, and walk-throughs are established to facilitate the completion of each deliverable review via the following process:

         a. Each deliverable is reviewed by DOM and must require formal written approval from DOM before acceptance of the deliverable. The Vendor must allow for a minimum ten business days per deliverable following receipt for DOM to review and document its findings, except as specified by DOM. Based on the review findings, DOM may accept the deliverable, reject portions of the deliverable, reject the complete deliverable, or require that revisions be made. The Vendor must make all modifications directed by DOM within ten days of receipt.

         b. Establishing and monitoring code and application standards and practices as integrated with any applicable State and project standards.

         c. Verifying requirements are well defined, understood, documented, and can be traced through design, development, and testing phases to verify the IDA Solution performs as intended.

         d. Ensuring SLA QA monitoring and associated reporting processes are established per this RFP.

   d. Security, Privacy, and Associated Laws

      1. Vendor must comply with Mississippi laws, guidelines, and standards for Substance Abuse/Mental Health-State Plan for Mental Health Services.

2. Vendor must comply with Mississippi laws, guidelines, and standards related to State Board of Pharmacy.

3. Vendor must comply with Mississippi law, guidelines, and standards related to State Board of Medical Licensure.

4. Vendor must comply with applicable CMS Requirements listed, but not limited to 45 CFR, 42 CFR, the State Medicaid Manual, 43 CFR, 1915 C-waivers, and 1905.

5. Vendor must comply with all Mississippi beneficiary privacy laws and manage specially protected data according to Mississippi law.

6. Vendor must comply with all applicable privacy and security standards.

7. Vendor and DOM must jointly define and adopt a set of privacy and security criteria to certify organizations for access to systems as necessary, such as the Provider Portal.

8. Vendor must comply with all regulations and best practices for physical and network security of health information, including but not limited to encryption in transit and encryption at rest for all systems and services, including all subcontractors and subcontractor software, hardware, and services. Encryption levels and formats shall be mutually agreed up on by DOM and the Vendor, with full disclosure of all subcontractors to DOM.

9. The proposed solution must support encryption at the database level, at the user device level, and during data transmission to secure the data in transit and at rest.

10. The IDA Project will contain the PHI of Medicaid beneficiaries, thus the proposed solution must comply with federal and state privacy laws, including HIPAA. Vendor compliance with HIPAA must include, but is not limited to, the following key HIPAA rules:

    a. Minimum Necessary: A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

    b. Access and Uses: Covered entities must develop and implement policies and procedures that restrict access and uses of PHI based on the specific roles of the members of their workforce.

    c. Disclosures and Requests for Disclosures: Covered entities must establish and implement policies and procedures (which may be standard protocols) for routine, recurring disclosures, or requests for disclosures, that limits the PHI disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure.

    d. Early Breach Detection and Notification: As defined by HIPAA, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI.

11. The proposed solution must have early detection and notification capabilities to notify the Vendor and DOM of a breach, along with following security and privacy protection capabilities.

12. The proposed solution must contain security and privacy capabilities. Business processes must have access requirements, data models, and technical models that address security and privacy capabilities. The technical capabilities must protect the existing DOM infrastructure against known threats and, as it evolves, respond to new threats via authentication, authorization, and encryption.

13. Security in the data models must include role and data element-based access control authorization.

14. Security must use configuration tools and business application functionality linked to common security mechanisms.

15. The proposed solution must establish security measures which, together with the Security Policy and Procedures, will provide PHI data confidentiality, integrity, and user accountability.

16. The proposed solution must support data security including both data encryption in transit and at rest.

17. The proposed solution must use Hypertext Transfer Protocol secured with TLS (HTTPS) for all Web Service encryption. The minimum requirement is HTTP 1.1 with TLS 1.2 or above for securing data transmissions.

18. The proposed solution should support VPN connections only for Vendor and support access to the solution as needed.

19. The proposed solution must provide a consistent approach to logging information with controls that can increase or decrease logging levels.

I. Change Order Process

113. DOM may wish to add functionality outside the scope of this RFP after the initial deployment of the awarded solution. Additional services will be provided through the Change Order process and will be approved as a not to exceed fixed price (calculated at a fully loaded hourly rate multiplied by the estimated number of hours to complete a proposed deliverable). Payment will be issued upon completion of the deliverable at an amount equal to or less than the proposed Change Order not-to-exceed price that reflects actual number of hours to complete the deliverable multiplied by the fully loaded hourly rate. Cost must be presented by role and by deliverable. These rates shall be used in the pricing of any subsequent change orders. Fully loaded rates include hourly rate plus travel, per diem, and lodging.

114. DOM will email a Change Order Request Form to the Vendor to provide services or resources that are not within the scope of this RFP. The Change Order Request will include:

    a. Description of the service or resources needed.

    b. Performance objectives and/or deliverables, as applicable.

    c. Due date and time for submitting a response to the request.

    d. Required place(s) where work must be performed.

115. Vendor must email a response to DOM within the specified time and include at a minimum:

a. A response that details the Vendor's understanding of the work.

b. An explanation of how tasks must be completed and a timeline for completion. This description must include proposed subcontractors and related tasks.

c. State resources (e.g., work site, and /or access to equipment, facilities, or personnel).

d. The proposed personnel resources, including any subcontractor personnel, to complete the task.

116. All Change Orders that require fixed price must be reviewed and approved by DOM. DOM will submit the Change Order to ITS for final approval. Based on the amount of the Change Order, ITS Board approval may be required.

117. Once the Change Order has been executed, the Change Order will be approved, and work may begin.

118. Vendor must provide fully loaded fixed on-site hourly rates for the services that they are responding to from this RFP, as well as fully loaded fixed off-site rates.

119. Vendor must describe the Change Order and staffing strategy.

120. Change Control Process

a. The Change Control Board (CCB) is a joint group with responsibility for all aspects of the IDA. The CCB will maintain a change control tracker.

b. Vendor must implement a change control tracking and reporting system that uniquely identifies the Vendor-related change control item with a tracking number, brief description, long description, disposition (e.g. pending, approved, deferred, rejected, deployed, etc.), proposed cost, estimate breakdown (i.e. hours and rate by labor category), priority (1-critical, 2-high, 3-medium, and 4-low), rank, reported by, assigned to, key dates (e.g. identified, submitted to DOM, approved by DOM, deployed, etc.), notes/comments, and other fields as mutually agreed upon by DOM and the Vendor.

c. Vendor must participate in CCB meetings conducted at least once per month or at DOM's request. The CCB will include DOM's Contract Monitor, DOM Project Manager, and representatives from key stakeholder groups, as unilaterally determined by DOM. Vendor will typically be represented by the Vendor Project Manager as the required CCB member. Other Vendor personnel must be made available to facilitate productive execution of the CCB. If the CCB does not agree on an item's classification as either a change request, clarification of a requirement, or a defect, DOM's determination must be final.

d. Vendor must follow the CCB process to request Technical Solution changes in advance. No change to the Technical Solution must be implemented without prior DOM approval of the concept, approach, impact assessment, and schedule.

e. Vendor must prepare for the CCB by compiling candidate hosting and/or operations related CCB items. The list of candidates CCB items must include enough information for the CCB to determine if the Vendor is required to formally submit a change request for an item.

f. The CCB must review proposed change requests. If approved, the Vendor must provide a target completion date and provide updates to DOM's Project Manager on all change requests that are in process.

g. Vendor must provide a Change Request Summary that includes the unique tracking number, short description, cost (if applicable), date submitted, date approved, status, approved date, completion date, and any relevant notes or comments. The Vendor must provide a summary of the total cost and quantity of all approved/deployed change requests. "No Cost" change requests are also to be submitted for review and approval by the CCB.

h. For all change control items that are implemented, the Vendor must provide a 45-business day post-launch warranty period where the change request is free of defects prior to billing for the item. Significant defects addressed during the warranty period reset the warranty period, based on the time they are fixed and implemented.

121. Vendor must provide sample documents with their RFP response for the Project Management Plan, Project Work Plan, Staffing Plan, Business Requirements and RTM, Communication Plan, Outreach Plan, and Software Architecture Design and Cloud Infrastructure Design documents.

III. OPTIONAL ANALYTICS

The inclusion of an analytics and population health module in the DOM EDL solution is optional for this RFP. Should the vendor choose to include this functionality, their response must address the requirements in this section. However, if analytics and population health tools will not be proposed as part of the solution or should the agency decide to not exercise the optional services, the Vendor should not respond to this section and the Vendor must ensure that their proposal is capable of providing the necessary data and interface functionality to accommodate such tools in the future in accordance with the requirements in this section. If this functionality is not included in the Vendor's original proposal, it cannot be added at a later time.

A. Analytics and Population Health

122. The new DOM State Medicaid Analytics and Population Health component must be integrated with the new DOM EDL and components outlined in this RFP.

123. Vendor may propose one or more analytics solutions.

124. Proposed solutions must be priced individually under optional software solutions in Section VIII, *Cost Information Submission*.

125. Solution should be a Software as a Service (SaaS) model; a cloud-based solution where the vendor is responsible for installing, hosting, and maintaining the system.

126. Vendor's production application and hardware shall be available 24 hours a day, 7 days a week excluding regular maintenance windows which must be approved by DOM. This also applies to failover and disaster recovery environments.

127. Vendor will notify DOM when application performance is likely to be impacted and will notify DOM at least 72 hours in advance of any maintenance outside of the approved regular maintenance windows. Any scheduled maintenance outside the regular maintenance window must be approved by DOM. There is a service level requirement of 99.9% availability.

128. The Analytics solution will provide DOM staff with scheduled and ad hoc report management, medical and program/service reports, and information using state-of-the-art analytics and reporting tools, including online reports and static reports

generated in a preformatted manner. Scheduled reports must be generated and available in a timely fashion.

129. The Analytics solution must have access to all data within the EDL, constrained only by access controls.

130. The Analytics solution must include anomaly detection functionality to identify patterns and outliers across multiple data groups, e.g., lines of business, member categories, or providers.

131. The Analytics solution must provide comparison capability of CCO performance in costs and quality, including against Fee for Service data using CCO Claims data sourced from the CCOs.

132. The Analytics solution must utilize disease registries for the management of disease states of the Medicaid Population.

133. The Analytics solution must provide the ability to segregate and analyze denied claims, including both Medicaid denied claims and CCO denied claims.

134. The Analytics solution must provide customizable data visualization options using multiple datasets.

135. The Analytics solution must provide ability to summarize, sort, group, aggregate, and filter. The solution must facilitate searches through large amounts of data, including claims data, clinical data, eligibility data, Social Determinants of Health (SDoH), and administrative data with specific focus on costs, utilization, and quality of care.

136. The Analytics solution must use beneficiaries' lock-in codes as required to identify key populations. Currently CAN (Coordinated Access Network) and CHIP (Children's Health Insurance Program) related data are necessary information. This includes lock-in begin date, end date, and provider for all beneficiaries enrolled in either program. Additional lock-in information for other programs must be available for ad hoc reporting.

137. The Analytics solution must include a set of standard report features. The Medicaid Analytics solution must provide flexible reporting tools and the ability to create and store customized reports.

138. Vendor will develop up to 10 standard analytics reports defined during the design and development phase which will be available as part of implementation. Vendor agrees to develop additional reports upon request.

139. The solution must allow export of reports in the following formats at a minimum:
    a. Excel (.xlsx)
    b. Comma-separated values (CSV)
    c. Adobe Portable Document Format (.pdf)

140. Exported reports in Excel and PDF formats should include a summary of report criteria, including run date, data filter details, and summary information (number of records, totals for summarized fields, etc.). Users should have the option to include or hide this information prior to export.

141. Exported reports should include an option to lock or password-protect reports prior to export.

142. The Analytics and Population Health solution should include the ability to create calculated fields, i.e., new fields for reporting based on logical tests or mathematical calculations based on existing fields.

143. The Analytics solution must be accessible using various browsers, at a minimum Internet Explorer 9.0, Microsoft Edge (no version dependency), and Firefox 3.0. The application is to be accessible by the supported Internet browsers, running on a computer with an operating system (Windows or Mac) capable of supporting those browsers. The application must be updated over time to support new versions of these browsers.

144. The Analytics solution must allow the import of data from disparate sources to allow Analytics to use both medical and socio-economic data. This data may reside within the DOM EDL or in external data stores.

145. The Analytics solution must allow for identification of specific Medicaid beneficiaries and populations, including by costs, quality, risk, disease state, and other DOM-defined parameters.

146. The Analytics solution must be user friendly to allow users with minimal technical training to utilize provided tools to perform the requested reporting functionality.

147. The Vendor must provide Training and Adoption Services support, as needed, either onsite or virtually.

148. The Analytics and Population Health solution must integrate with Terminology Services.

149. The solution must provide overall administrative functionality using a Graphical User Interface (GUI).

150. The Analytics and Population Health Vendor must provide responsive user support with a clear escalation plan.

151. All access to PHI must be recorded and made available for reporting to include the following, at a minimum:

    a. Timestamp
    b. Content accessed
    c. Person accessing
    d. Physical location of access with IP address
    e. Reason for access
    f. Method of access

    This information will be available to DOM staff, auditors, and HIPAA reporting/auditing requests.

152. The solution must prohibit unauthorized users from accessing PHI and other sensitive information according to State and Federal confidentiality rules.

153. Vendor staff (including development and support staff) must use two factor authentication when accessing any aspect of the production application or its data.

154. The Analytics and Population Health solution must include functionality so that it isolates and does not display data on non-Medicaid beneficiaries.

155. Vendor must document the design and algorithms for each analytic report.

156. Vendor must document and carry out QA processes to ensure the accuracy of each report.

157. Vendor must fully document all aspects of the solution and must, throughout the life of the contract, maintain and update on a regular basis all documentation to reflect the current state of the application(s), including a data dictionary. A data dictionary example must be included with the RFP response.

158. Although ICD-10 codes went into effect on October 1, 2015, DOM will continue to house ICD-9 data. The proposed Vendor must be able to display such data in the form in which it was received. In addition, ICD-11 codes shall be accommodated when the standard is implemented. All ICD code data will remain housed throughout the term of the Vendor contract.

159. The Medicaid Analytics and Population Health solution must interface with the Sensitive Codes solution and must return only that data appropriate to the security level of the user.

160. The Population Health Solution must provide physician and provider performance reports, including custom DOM reports on costs and quality of care.

161. The Population Health Solution must provide, at a minimum, disease risk stratification and analysis, population level dashboards, identification of care opportunities, beneficiary outcome reporting and analysis, and gaps in care reporting and analysis.

162. Proposed solutions must include predictive modeling capabilities, risk scoring, and the ability to quickly develop real time analytics analysis from all data in the DOM EDL.

163. Proposed solution must include self-serve user-friendly data science capabilities to build, train and deploy various machine learning models as well as forecasting (time series) models from structured and unstructured data housed in the DOM EDL.

164. The DOM State Medicaid Analytics and Population Health Management Initiatives must follow Industry Standards and Best Practices.

165. Vendor has the option to bid on an Electronic Clinical Quality Measures (eCQM) solution if they so choose.

166. The Medicaid eCQM solution must provide Medicaid-specific quality measurement reporting and analysis based on Office of National Coordinator of Health Information Technology (ONC) and the CMS rules, standards, and certifications. (Providing HEDIS quality reporting is not sufficient and will not meet this requirement.) https://www.medicaid.gov/medicaid/quality-of-care/quality-of-care-performance-measurement/index.html

167. The eCQM solution must be an ONC Certified eCQM solution.

168. The eCQM solution must be hosted as a SaaS solution.

169. The eCQM solution must support all clinical quality measures supported by the ONC and/or CMS, and support both the individual and population level of reporting.

170. The eCQM solution must have a development and production environment, as well as a DR environment.

171. The eCQM solution must have a reporting engine allowing custom reports to be generated and delivered, including graphics-based reports (on demand), including at the patient level, provider level, and state level.

172. The eCQM solution must support QRDA, C-CDA, and FHIR/USCDI data formats.

173. The eCQM solution must include training, documentation, and support for DOM users.

IV. SOFTWARE ADMINISTRATION AND SECURITY

A. Cloud or Offsite Hosting Requirements

174. Data Ownership

    a. DOM shall own all right, title and interest in all data used by, resulting from, and collected using the services provided. The Vendor shall not access DOM User accounts, or DOM Data, except (i) in the course of Data Center operation related to this solution; (ii) response to service or technical issues; (iii) as required by the express terms of this service; or (iv) at DOM's written request.

    b. Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Vendor to ensure that there is no inappropriate or unauthorized use of DOM information at any time. Vendor shall safeguard the confidentiality, integrity, and availability of DOM information and comply with the following conditions:

        1. All information obtained by the Vendor under the contract shall become and remain property of DOM.

        2. All documents developed by the Vendor under the contract shall become and remain property of DOM, including technical design, user guide, QA records, meeting minutes, etc.

        3. At no time shall any data or processes which either belong to or are intended for the use of DOM or its officers, agents, or employees be copied, disclosed, or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include DOM.

175. Data Location

    a. Vendor shall not store or transfer DOM data outside of the continental United States. This includes backup data and DR locations. The Vendor will permit its personnel and contractors to access DOM data remotely only as required to provide technical support.

176. Encryption

    a. Vendor must encrypt all non-public data in transit regardless of the transit mechanism.

    b. For engagements where the Vendor stores non-public data, the data shall be encrypted at rest. The key location and other key management details will be discussed and negotiated by both parties.

    c. Where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection.

  d. If the Vendor cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. The policy shall comply with the following requirements.

   1. The policy shall be issued by an insurance company acceptable to DOM and valid for the entire term of the contract, inclusive of any term extension(s).

   2. Vendor and DOM shall reach an agreement on the level of liability insurance coverage required.

   3. The policy shall include, but not be limited to, coverage for liabilities arising out of premises, operations, independent contractors, products, completed operations, and liability assumed under an insured contract.

   4. At a minimum, the policy shall include third party coverage for credit monitoring, notification costs to data breach victims, and regulatory penalties and fines.

   5. The policy shall apply separately to each insured against whom claim is made or suit is brought subject to the Vendor's limit of liability.

   6. The policy shall include a provision requiring that the policy cannot be cancelled without 30 days written notice.

   7. Vendor shall be responsible for any deductible or self-insured retention contained in the insurance policy.

   8. The coverage under the policy shall be primary and not in excess to any other insurance carried by the Vendor.

   9. In the event the Vendor fails to keep in effect at all times, the insurance coverage required by this provision, DOM may, in addition to any other remedies it may have, terminate the contract upon the occurrence of such event, subject to the provisions of the contract.

177. Breach Notification and Recovery

  a. Unauthorized access or disclosure of non-public data is considered to be a security breach. The Vendor will provide notification within 4 hours of the incident and all communication shall be coordinated with DOM. When the Vendor or their sub-contractors are liable for the loss, the Vendor shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least three years, mailing costs, website, and toll-free telephone call center services. DOM shall not agree to any limitation on liability that relieves a Vendor from its own negligence or to the extent that it creates an obligation on the part of DOM to hold a Vendor harmless.

178. Notification of Legal Requests

  a. Vendor shall contact DOM immediately upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of DOM. The Vendor shall not respond to subpoenas, service of process, and other legal requests related to DOM without first notifying DOM unless prohibited by law from providing such notice.

179. Termination and Suspension of Service

a. In the event of termination of the contract, the Vendor shall implement an orderly return of DOM data in CSV or XML or another mutually agreeable format. The Vendor shall guarantee the subsequent secure disposal of DOM data.

b. Suspension of services: During any period of suspension of this Agreement, for whatever reason, the Vendor shall not take any action to intentionally erase any DOM data.

c. Termination of any services or agreement in entirety: In the event of termination of any services or of the agreement in its entirety, the Vendor shall not take any action to intentionally erase any DOM data for a period of 90 days after the effective date of the termination. After such 90-day period, the Vendor shall have no obligation to maintain or provide any DOM data and shall thereafter, unless legally prohibited, dispose of all DOM data in its systems or otherwise in its possession or under its control. Within this 90-day timeframe, Vendor will continue to secure and back up DOM data covered under the contract.

d. Post-Termination Assistance: DOM shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement.

e. Secure Data Disposal: When requested by DOM, the provider shall destroy all requested data in all its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to NIST approved methods. Certificates of destruction shall be provided to DOM.

180. Background Checks

   a. Vendor warrants that it will not utilize any staff members, including sub-contractors, to fulfill the obligations of the contract who have been convicted of any crime of dishonesty. The Vendor shall promote and maintain an awareness of the importance of securing DOM's information among the Vendor's employees and agents.

181. Security Logs and Reports

   a. Vendor shall allow DOM access to system security logs that affect this engagement, its data, and/or processes. This includes the ability to request a report of the activities that a specific user or administrator accessed over a specified period of time as well as the ability for an agency customer to request reports of activities of a specific user associated with that agency. These mechanisms should be defined up front and be available for the entire length of the Agreement with the Vendor.

182. Contract Audit

   a. Vendor shall allow DOM to audit conformance including contract terms, system security, and Data Centers as appropriate. DOM may perform this audit or contract with a third party at its discretion at DOM's expense.

183. Sub-contractor Disclosure

   a. Vendor shall identify all its strategic business partners related to services provided under the contract, including but not limited to, all subcontractors or

other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.

184. Sub-contractor Compliance

   a. Vendor must ensure that any agent, including a Vendor or subcontractor, to whom the Vendor provides access agrees to the same restrictions and conditions that apply through this Agreement.

185. Processes and Procedures

   a. Vendor shall disclose its non-proprietary security processes and technical limitations to DOM so that DOM can determine if and how adequate protection and flexibility can be attained between DOM and the Vendor. For example: virus checking and port scanning. DOM and the Vendor shall work together to understand each other's roles and responsibilities.

186. Operational Metrics

   a. Vendor and DOM shall reach an agreement on operational metrics and document said metrics in the Service Level Agreement (SLA). At a minimum, the SLA shall include:
      1. Advance notice and change control for major upgrades and system changes
      2. System availability/uptime guarantee/agreed-upon maintenance downtime
      3. Recovery Time Objective/Recovery Point Objective
      4. Security Vulnerability Scanning

B. Project Milestones

187. DOM will work with the awarded Vendor to determine overall project and payment milestones. At a minimum they will include:

   a. DOM acceptance of the Project Team and Project Plan.
   b. Successful UAT of all components.
   c. Training and acceptance of documentation.

188. IDA component payment milestones:

   a. DOM acceptance of the EDL Architecture and Design and Integration design.
   b. DOM acceptance of the IDA Populations tools, Architecture, and design.
   c. DOM acceptance of the IDA Controls and Management tools, Architecture, and design.
   d. DOM acceptance of the IDA Data Gateway Architecture Design including Centralized data access control, Interfaces, Transaction management, Load Balancing/High Availability, and Data Cleansing.
   e. DOM acceptance of the integration design for the EMPI.
   f. DOM acceptance of the integration design for the Opt Out, Sensitive code processing, and HLI processing.
   g. DOM acceptance of the API Architecture and Design and integration design.
   h. DOM acceptance of the Interoperability Architecture and Design.
   i. DOM acceptance of the historic load of claims data to the Data Lake.

j. DOM acceptance of the load of historic C-CDAs to the Data Lake.

k. DOM acceptance of the load of current beneficiary data to the Data Lake.

l. DOM acceptance of the API applications and tools.

m. DOM acceptance of all IDA support components.

n. Delivery of all components of the IDA Solution to the DOM approved Data Center or cloud solution.

o. Go-live of all components of the EDL Infrastructure and Applications.

C. Planning for the Future

189. The DOM IDA solution must be scalable to support both data storage and application performance for new requirements as they are identified. Examples:

a. There is currently a separate database populated to support Transformed Medicaid Statistical Information System (T-MSIS) processes. DOM anticipates this functionality being imported to the new DOM EDL. For this phase, T-MSIS support is out of scope; however, DOM is requesting an optional, separate price to migrate this functionality from the currently existing data warehouse and into the EDL as part of a potential phase 2. Please provide this optional, separate pricing in Section VIII: *Cost Information Submission* of the RFP.

b. The existing DOM Data Warehouse solution currently supports more than 6,000 reports. DOM anticipates that many of these reports will eventually be modified to utilize data from the new DOM EDL. For this phase, this is out of scope; however, DOM is requesting an optional price to migrate this functionality from the currently existing data warehouse and into the EDL as part of a potential phase 2.

c. DOM plans to engage a Systems Integrator (SI) to assist with the strategy and implementation of future initiatives. The IDA Vendor will be required to work with this SI during latter phases of the IDA project.

d. DOM will be replacing the current DOM Interoperability Platform ESB provided by Gainwell Technologies with a new DOM Integration Platform. This integration platform is expected to provide ESB services, Data Governance services, Identity Management services, and other services. Migration to the new platform is anticipated to take place in late 2023 or early 2024. The IDA Vendor will be required to integrate with the new DOM Interoperability platform when it is implemented, using an interface as specified in this RFP, at no additional cost.

190. Data Virtualization (DV)

a. Vendor must build a DV capability in the EDL for adopting auxiliary data, scattered data, and infrequently used data to provide DOM with a complete data view of the EDL.

V. FINAL ACCEPTANCE REVIEW

191. Vendor agrees that upon the successful completion of all implementation phases, including end user training, DOM will conduct a Final Acceptance Review (FAR) to determine whether or not Vendor has satisfied the terms and conditions of the awarded contract, which includes the requirements of RFP No. 4243, and Attachment A.

VI.   SUPPORT AND MAINTENANCE

The SLAs set forth herein shall be in effect beginning with the commencement of monthly services. The Vendor shall be responsible for complying with all performance measurements and ensure compliance by all subcontractors.

Beginning on the SLA activation date, if any performance measurement is not met during the monthly reporting period, the SLA credit for that individual measurement shall be applied to the monthly fees.

A. Service Level Agreements (SLA):

192. System Availability – The Vendor's proposed solution must operate 24 hours a day, and support a 99.9% uptime per month, and is subject to up to a $5,000.00 penalty for each occurrence of downtime outside of the 99.9% uptime requirement. Uptime must be calculated by the following formula:

    24 hours per day x 7 days a week x 52 weeks per year = Total hours per year.

    Total hours per year x .001 = Allowed unscheduled downtime per year.

Table 1 - SLA

Uptime Range	Associated Down Time	Penalty Per Component or Interface	Penalty for Entire Solution Downtime
99.5-99.8%	43.69 mins -3.6 hrs.	$2,500.00	$10,000.00
99.0-99.4%	3.7 hrs. -7.3 hrs.	$4,000.00	$15,000.00
98.0-98.9%	7.4 hrs. – 14.6 hrs.	$6,000.00	$25,000.00
Below 98%	>14.6 hrs.	$9,000.00	$35,000.00

193. Allowed unscheduled downtime per year/12 = Allowed unscheduled downtime per month. (Multiply by 60 to convert to minute).

194. Solution downtime outside of the allowable downtime period must be categorized as unscheduled downtime and is subject to a $10,000.00 penalty for each occurrence.

195. System Maintenance: Scheduled downtime equals the aggregate total of all hours of planned and scheduled maintenance performed during the month. Any scheduled downtime exceeding this agreed upon amount must be deemed as unscheduled downtime for purposes of measuring system performance.

196. Scheduled solution downtime must occur between 1:00 a.m. and 4:00 a.m. Central Time, and only with prior, written approval from the State 48 hours in advance. Vendor will be assessed a penalty of $5,000.00 per instance of a failure to notify the State in writing 48 hours in advance of a scheduled downtime. Solution downtime outside of the allowable downtime period shall be categorized as unscheduled downtime and is subject to a $10,000.00 penalty for each occurrence.

197. Failure to annually meet the latest version of CMS MARS-E and attest to a MARS-E compliant environment is subject to a $10,000.00 penalty, with a $2,500.00 for each additional month out of compliance.

198. Vendor must adhere to the following table for severity of incidents and associated penalties (credit to DOM):

Category	Description	Resolution	SLA Penalty
Severity 1*	A Severity 1 incident represents a complete loss of service or a significant feature that is completely unavailable or non-operational for all users of the system and no workaround exists.	Severity 1 incidents, which are not code related or external network failure shall be corrected within 2 hours or within a mutually agreed upon time period (cure period), otherwise the Severity 1 incident shall be corrected within 4 hours or within a mutually agreed upon time period (cure period).	Up to $5,000 for each calendar day beyond the applicable cure deadline not to exceed $25,000 per incident. Applicable penalties will be assessed monthly.
Severity 2	A Severity 2 incident represents a partial loss of service with severe impact for all users of the system and no work-around exists.	Severity 2 incidents which are not caused by capacity issues or backup site availability shall be corrected within 4 hours or within a mutually agreed upon time period (cure period), otherwise the Severity 2 incident shall be corrected within 8 hours or within a mutually agreed upon time period (cure period).	Up to $1,000 for each calendar day beyond the applicable cure deadline not to exceed $5,000 per incident. Applicable penalties will be assessed monthly
Severity 3	A Severity 3 incident represents a minor loss of service. The result is an inconvenience, which may require a temporary workaround.	Severity 3 incidents shall be corrected within 3 days or within a mutually agreed upon time period (cure period).	$250 for each calendar day beyond the applicable cure deadline not to exceed $1,500 per incident. Applicable penalties will be assessed monthly.

Severity 4	A Severity 4 incident represents no loss of service. The result does not prevent operation of the software. An example of a Severity 4 could be a client facing error.	Severity 4 incidents shall be corrected within 5 days or within a mutually agreed upon time period (cure period).	$125 for each calendar day beyond the applicable cure deadline not to exceed $625 per incident. Applicable penalties will be assessed monthly.

*For severity 1 issues, the root cause analysis document must be provided within 5 working days from day of resolution.

B. Operations:

199. Vendor must adhere to the following table for SLAs and associated penalties (credit to DOM):

Table 2 – Service Credit Assessments

Service Requirement	Measurement	SLA	SLA Credit
Problem Resolution Time – High	Resolution Time for each High Priority Problem. Problem resolution time is defined as the period from when the issue is reported to when it is properly resolved.	98% <4 hours	−$8,000
Problem Resolution Time - Normal	Resolution Time for Normal Priority Problems	98% <24 hours	−$8,000
Problem Resolution Time - Low	Resolution Time for Low Priority Problems	98% <72 hours	$8,000
Help Desk Operations - Daily Email & Voicemail	Time for Help Desk to Create a Ticket from Email or Voicemail notification (90% goal)	90% <1 business day	$8,000
Help Desk Operations - Backlog Email & Voicemail	Time for Help Desk to Create a Ticket from Email or Voicemail notification (98% goal)	98% <3 business days	$16,000

Service Requirement	Measurement	SLA	SLA Credit
IDA Recovery	In the event of a declared disaster the recovery time objective is forty-eight (48) hours. The system should be fully operation and available. The SLA Credits for this Measurement are aggregated, i.e., each lower level of failure adds the stated additional percentage (for a maximum 50% credit at the lowest level).	<48 hours	$30,000
		<72 hours	+$45,000
		<96 hours	+$75,000

200. Data Integrations with Medicaid Trading Partners failed transactions: Any failure of transactions to or from Medicaid Trading Partners that is above a daily total of 2.5% of the daily transaction total shall be subject to a penalty of $1,000.00 per daily occurrence. Any failure of transactions to or from Medicaid Trading Partners that is above a monthly total of 1.0% of the monthly transaction totals must be subject to a penalty of up to $5,000.00 per monthly occurrence.

201. All maintenance and enhancement hours must have prior approval by DOM.

C. Performance Requirements:

202. As each component has a user interface (GUI), each component must support a five second or less average for each of these processes.

   a. The user login,
   b. Single patient query and return results,
   c. Building and delivering a data file to the user,
   d. Standard report generation (some reports, may take longer than the required five seconds to generate, and if so, please note in your response what reports these are, the data sets and size that are typically included, and the estimated performance for generating these reports), and
   e. Averages of more than five seconds will be considered an outage and the Vendor must be assessed damages of $2,500.00 per day.

D. Disaster Recovery

203. Licensor shall host the proposed solution in a United States-based Tier 2 data center or better, with written approval from the State on any change in the selection of the data center, data center Vendor, and location. The State reserves the right to physically audit (by State or State contracted personnel) the data center the proposed solution is hosted in and the DR site. By the first 90 days after contract execution and on every August 30th thereafter, the Licensor must provide the State with an annual data center report, specifying their Tier Certification of Constructed Facility rating or TIA-942 Data Center Standard Rating, specifying the Tier rating of their facility and specifying what certifications have been awarded to the facility, including but not limited to LEED, SSAE 16, HIPAA, etc. Failure to provide an annual report is subject to a penalty of up to $50,000 per month until the report is completed and provided to the State.

204. Data center-provided servers and network switching equipment used to host the proposed solution shall be no more than three (3) years old, and hardware shall be regularly scheduled for an equipment refresh every three (3) years. Failure to refresh this hardware at least every three (3) years and to notify the State in writing as to this refresh is subject to a penalty of up to $50,000 per month until the refresh is complete, and the State is notified.

205. Data center where all instances are hosted shall have system intrusion detection, firewalls and firewall policies for cloud servers, regular OS security patches, the most current antivirus software installed, and follow hosting / data center best practices. Upon contract execution, and every quarter thereafter, the Licensor shall provide the State a quarterly report detailing how the Licensor and data center are adhering to these requirements. Failure to provide an annual report is subject to a penalty of up to $50,000 per month until the report is completed and provided to the State.

206. Vendor must have a DR plan, including a separate DR site with a separate physical location from the primary hosting site. Upon contract execution, the Vendor must provide documentation that the DR environmental test has been conducted within the past year and must provide written results to the State. The written results must include any remediation and the accompanying remediation schedule necessary to correct any failures or findings that were identified as a result of the DR test. Failure to provide the results to the State on an annual basis is subject to a penalty of up to $50,000.00 per month until the report is completed and provided to the State.

207. Vendor must execute the DR plan immediately upon notification of a Disaster (as outlined in the DR plan). Upon execution of the DR plan, the solution and data must return to at least 70% performance status of the production status. Failure to provide at least 70% performance status of the production status is subject to a penalty of up to $50,000.00 per month until at least 70% performance status is complete, and documentation is provided to the State.

208. Vendor must support a zero Recovery Point Objective (RPO), exclusive of a declared disaster event. Failure to provide zero RPO is subject to a penalty of up to $50,000.00 per month until a zero RPO is completed, and documentation is provided to the State.

E. Privacy and Security

209. Vendor and all subcontractors must adhere to the appropriate SLAs. Any and all subcontractor non-performance and delays are the responsibility of the prime Vendor, and all penalties will be assessed to the prime Vendor.

210. If any Vendor or any subcontractor fails to meet the requirements of the Business Associate Agreement (BAA) or Data Use Agreement (DUA), the Vendor shall be assessed a penalty of $2,500.00 per occurrence. An occurrence means each failure to comply with the BAA or DUA requirements, regardless of the number of persons or clinicians involved.

211. If any Vendor or subcontractor fails to notify the State of a breach (potential or otherwise) both in writing and by telephone within 24 hours of discovery, the Vendor shall be assessed damages of up to $25,000.00 per calendar day until the State is properly notified. The Vendor must pay the costs for notification of any breach, as

well as for credit monitoring for all persons whose data is breached for the term of one year.

F. Vendor Reporting Requirements and Penalties

212. The Vendor must provide a monthly report to the State by the seventh business day of the following month. Failure to provide the monthly report by the seventh working day of the following month, the Licensor shall be assessed a penalty of up to $2,500 per calendar day until the report is delivered. Report should include:

    a. Component performance metrics by component and all Data Integration performance metrics including failed transactions.
    b. Internal monitoring of the EDL, including metrics and tools used.
    c. Incidents (problems) incurred per defined SLAs.
    d. Provider user metrics (number of active and inactive users for Provider Access, user logins, user queries, etc.).
    e. Data Integration queries, responses, bi-directional data transmissions by integration type other queries and responses), etc.
    f. EDL and Data Integration uptime.
    g. Bandwidth metrics of the EDL.
    h. Hardware status of the EDL.
    i. Response times for interaction with the new EMPI from Verato.
    j. Total ticket volume with aging, tickets opened and closed during the last period, by support, maintenance, and upgrades.
    k. Daily test results of the performance of the Provider Portal. The daily test results on the performance of the Provider Portal will be reported to DOM in the monthly report.
    l. Monthly hardware statistics and monitoring reports.
    m. Other metrics to be defined by the State in coordination with the Vendor. If the Vendor does not provide the monthly report by the seventh working day of the following month, the Vendor shall be assessed a penalty of $2,500.00 per month until the report is delivered.

213. Should any Vendor have 50 or more unresolved Help Desk tickets that average in excess of 72 hours from submission, the Vendor is subject to a penalty of up to $2,500.00 per calendar day.

214. Failure by any Vendor to meet mutually agreed upon deliverables and/or milestones by the due date or as otherwise required, may result in a penalty of up to $2,500.00 per instance, per calendar day that the deliverable or milestone remains late or deficient.

215. Failure by any Vendor to maintain staffing levels, including the number and qualifications of staff, and provision of key positions that are outlined in the contract, is subject to a penalty of up to $5,000.00 per instance, per calendar day.

216. Vendor must provide the State a quarterly report detailing how the Vendor and datacenter are adhering to hosting requirements set forth in RFP and contract. These requirements. Failure to provide a quarterly report is subject to a penalty of up to $50,000.00 per month until the report is completed and provided to the State.

217. Vendor must have a failover process and documented failover plan that must be provided to the State. Failure to provide the failover plan may result in a penalty of up to $50,000.00 per month until the report is completed and provided to the State.

218. Any other failure of any Vendor that DOM determines constitutes non-compliance with any material term of the Contract not specifically enumerated herein, may result in a penalty of up to $10,000.00 per instance, per calendar day.

219. Failure by the Vendor to obtain approval in writing by the Division of Medicaid for publishing material requiring DOM approval. This may result in $5,000.00 per instance, per calendar day.

220. Unauthorized use of DOM's name, brand, or likeness in violation of the contract may result in $1,000.00 per occurrence. An occurrence means each unauthorized use.

221. Failure of Vendor to comply with close out and turnover requirements may result in the assessment of damages of up to $20,000.00 per calendar day that, if imposed, shall be deducted from the final payment to be made to Vendor.

222. Unauthorized utilization of any data, in violation of the requirements of this RFP may result in $10,000.00 per occurrence. An occurrence means each unauthorized use, regardless of the number of beneficiaries or Trading Partners involved.

223. Failure to meet the requirements of Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Health Information Technology for Economic and Clinical Health Act (HITECH), and the implementing regulations thereunder, including but not limited to the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and 164, as amended (between $1,000 and $100,000 per incident, per calendar day). An incident means, with respect to protected health information (PHI), (i) any successful Security Incident which results in or is related to unauthorized access, use or disclosure of PHI, (ii) Breach of Unsecured PHI, or (iii) any loss, destruction, alteration or other event in which PHI cannot be accounted for.

224. Any other failure of Vendor that DOM determines constitutes non-compliance with any material term of the contract and/or RFP not specifically enumerated herein may result in an amount of up to $5,000.00 for each failure.

225. The Vendor shall publish on their public website any actual or liquidated damages that have been paid by Licensor within fifteen (15) business days of Licensor having paid such actual or liquidated damages, where such payment will only occur after notice of DOM approval and maintain the document on the site through the contract term.

226. If an SLA measurement yields an SLA credit, the Vendor must conduct a root cause analysis (RCA). Such root cause analysis must be provided to DOM within 5 business days of the outage event for DOM review and acceptance.

G. Liquidated Damages and Corrective Action Plans

227. DOM may require corrective action if any deliverable, report, SLA, or the like should indicate that the Vendor is not in compliance with any provision of the Contract. DOM may also require the modification of any policies or procedures of the Vendor relating to the fulfillment of its obligations pursuant to the Contract. DOM may issue a deficiency notice and may require a Corrective Action Plan (CAP) be filed within

15 calendar days following the date of the notice. A CAP shall delineate the time and way each deficiency is to be corrected. The CAP shall be subject to approval by DOM, which may accept it as submitted, accept it with specified modifications, or reject it. DOM may extend or reduce the time frame for corrective action depending on the nature of the deficiency and shall be entitled to exercise any other right or remedy available to it, whether it issues a deficiency notice or provides Vendor with the opportunity to take corrective action.

228.   Because performance failures by the Vendor may cause DOM to incur additional administrative costs that are difficult to compute, DOM may assess liquidated damages against the Vendor pursuant to this section and deduct the amount of the damages from any payments due the Vendor. DOM, at its sole discretion, may establish an installment deduction plan for any damages. The determination of the monetary amount of damages shall be at the sole discretion of DOM, within the ranges set forth below. Self-reporting by the Vendor will be taken into consideration in determining the monetary amount of damages to be assessed. Unless specified otherwise, DOM shall give written notice to the Vendor of the failure that might result in the assessment of damages and the proposed amount of the damages. The Vendor shall have 15 calendar days from the date of the notice in which to dispute DOM's determination. DOM may assess damages for specific performance failures set forth below. DOM may assess higher liquidated damages amounts when the Vendor consistently fails to meet specific performance standards and the deficient performance has not been corrected.

229.   Assessment of actual or liquidated damages does not waive any other remedies available to DOM pursuant to the contract or State and Federal law. If liquidated damages are known to be insufficient, then DOM has the right to pursue actual damages.

230.   Failure to timely submit a DOM approved CAP, DOM may assess liquidated damages of up to $2,500.00 per business day until the CAP is submitted.

231.   Failure to successfully carry out a DOM approved CAP within the time frames outlined in the CAP, DOM may assess up to $5,000.00 per business day until the CAP is completed.

232.   In the event of repeated violations of a single SLA measure or multiple failures across SLA measures over two consecutive months, the State reserves the right to renegotiate SLA measures and/or escalate the applicable reductions by 50% of the stated liquidated damages after non-responsiveness. Repeated violations may be grounds for Termination for Cause.